*Wikimedia Foundation v. NSA*
No. 15-cv-0062-TSE (D. Md.)

# Plaintiff’s Exhibit 13

English Not logged in Talk Contributions Create account Log in

WIKIMEDIA
META-WIKI

Content page Discussion Read Edit Add topic View history Search Meta Go

Main page
Wikimedia News
Translations
Recent changes
Random page
Help
Babel

Community

Wikimedia Resource Center
Wikimedia Forum
Mailing lists
Requests
Babylon
Reports
Research
Planet Wikimedia

Beyond the Web

Meet Wikimedians
Events
Movement affiliates
Donate

Print/export

Create a book
Download as PDF
Printable version

Tools

What links here
Related changes
Special pages
Permanent link
Page information
Link by ID

# Talk:PRISM

*The following discussion is closed.* ***Please do not modify it.*** *Subsequent comments should be made in a new section. A summary of the conclusions reached follows.*

**Based on the discussion below, the WMF legal team feels that there is general support for some PRISM-related action. However, we feel that the current proposals are either not strongly supported, or there are genuine concerns or reservations about them. The team will therefore continue to monitor the situation. In particular, in keeping with the consultation below, we will look for opportunities for action and collaboration that are:**

- **Focused on the movement's mission and values - for example, actions focused on ensuring reader privacy, or on protecting WMF's right to be transparent with the community**
- **Consistent with our international nature - in other words, actions that do not not privilege one country's citizens over another**

**We also recognize the questions and concerns raised here about privacy, and urge interested community members to continue that discussion as part of our larger privacy policy call for input.**

**Thanks to everyone who participated in the consultation. We encourage further discussion, including suggestion of potential actions, either through the new section at the end of this page, or through the advocacy-advisors list.**

LVilla (WMF) (talk) 21:34, 11 July 2013 (UTC)

**Contents** [hide]

## What wasn't said [edit]

This statement appears to carefully avoid speaking to the ongoing surveillance and traffic interception which Wikimedia has specific knowledge of but which itself is not actually an active party to, I think this is unfortunate and misleading.

I also note that the claims that Wikimedia has 'not “changed” our systems to make government surveillance easier' is, in my well informed opinion, basically a lie by omission: By failing to move all reader traffic to SSL wikimedia has failed to change its systems in order to limit the ongoing traffic observation and manipulation which it is specifically aware of (and, generally, to also protect against additional surveillance which Wikimedia may not be aware of). Because the traffic is unencrypted there would be little reason for any government to seek out Wikimedia's cooperation. With no active involvement required Wikimedia would have no opportunity to oppose blanket surveillance in a court of law. Evening ignoring the fact that Wikimedia is already aware that its traffic is being intercepted the use of SSL is a best practice which is already employed by default for all users on many popular websites.

It is my personal experience that in the past Wikimedia has not considered the privacy of its readers to be a high priority. I have never quite been able to understand why: My view has always been that to many people Wikipedia is an extension of their mind and their access patterns betray some of their most personal and intimate thoughts. But whatever the reason, adopting best practices to protect reader privacy has simply not been a priority and I've accepted that although I did not agree with it. But now I'm confused with the manner in which this post fails to acknowledge this past indifference while simultaneously claiming to care deeply. I would be delighted to hear that there was a change in priorities here, but considering the history it seems like this is simply a politically expedient response to a fad issue which will soon be forgotten. --Gmaxwell (talk) 00:45, 15 June 2013 (UTC)

> This certainly seems like a fad issue. While I'm not sure I'd characterize the lack of forced SSL in the same way you do, I think working on documents such as User:Sue Gardner/Wikimedia Foundation Guiding Principles is a much better use of time and other resources. This allows us to define what we stand for and what we believe, rather than

simply denouncing whatever the latest government abuse (or potential future abuse) happens to be in the news at the moment (SOPA, PRISM, etc.).

For what it's worth, bugzilla:47832 is the relevant bug about enabling HTTPS for all users. I doubt we'll see this happen this year or next, though.

And, at some level, there is a reasonable argument that some level of user responsibility is warranted. That is, stable HTTPS access (using pretty URLs) is currently available to anyone interested in using it. --MZMcBride (talk) 04:01, 15 June 2013 (UTC)

> well ssl is important, and I wish it was on all the time, i don't think it quite provides the protection you think it does. People can still do fingerprinting based on size of things requested. If you edit, the exact timestamp is recorded, which if the government is monitoring all the inbound ssl trafic should be enough to match you up to who you are. (Ssl only protects the content of the message. Not who sent it or that a message was sent. In the context of wikimedia where the message is already known or is public (usually), this isnt a lot of protection. (The biggest benefit in our context is protection against shared session attacks).Bawolff (talk) 15:27, 15 June 2013 (UTC)

SSL or TLS ? Which versions are supported, which one are deprecated and its support should be removed ? verdy_p (talk) 16:33, 15 June 2013 (UTC)

> Well this conversation is talking about encrypting http in general. Which version of SSL/TLS and if it is secure, is an implementation detail (An important implementation detail no doubt, but still off topic). Wikipedia apparently supports SSL3 and TLS1.0 according to https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org Bawolff (talk) 19:07, 15 June 2013 (UTC)

Hello Greg, can you say more about this surveillance and interception? Are you talking about datacenter-level or backbone-level surveillance?

And yes, let's finish enabling HTTPS by default for everyone. I don't see anyone suggesting obstacles to making that happen, other the observation that it hasn't happened yet. The comments on the relevant bugs seem to be ideas or positive reactions. And speeding the transition to SSL-only serviceis one effective way we can swiftly increase reader privacy, regardless of what is in our public statements of principle. –SJ talk 23:48, 15 June 2013 (UTC)

Even having https by default it would not be efficient for most of people: if users use a navigator which collect data. In this case, the software send statistics with "listening" on the input and output data, even with a SSL layer. Information are sent encrypted to the developper company. I espescially think to google chrome and it's HTTPs everywhere feature: "Nobody" can sniff data; except google. It is probaly the same with IE; safari etc... It is possible to think that they can send passwords if the user choose to record them

The use of some add-on can create the same problem.

Some Os (espescially mobile one) send data by simply check-in a develloper company server. I think to android which do things like time tracking per application. This make difficult to understand why nobody tried to create a build with stat funtion removed from android source code. Apple doesn't seems to collect data with OSx. It dosen't prevent to do this with iOS.

So instoring encryption by default aiming at spying programs would only have the effect to slow down connection with SSL headers, most of the time. It is useless until users of such software or OS recieve a warning banner. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 01:02, 16 June 2013 (UTC)

- **Comment** SSL is good for concealing stuff like passwords, but it's of no help for keeping private what articles people are reading, since the message lengths are usually enough to identify articles even if the packets are encrypted. Adding some random padding to each message before encryption can fuzz this up a litle bit, but not enough to matter. Also, Firefox 20 (I haven't tested other browsers) sends an OCSP request to Digicert (iirc) whenever you view an article on the secure site. That means Digicert gets the IP address of everyone who reads Wikipedia through SSL, which doesn't seem so great, although OCSP in general is a good idea. 50.0.136.106 07:21, 20 June 2013 (UTC)

  > The OCSP request is not very helpful to determine what you are reading. In fact, since we have now SUL activated by default, the secure connection can be proxied from a random site owned by the WMF, and unrelated to the wiki you are actually reading (that secure proxy can then be used to visit all Wikimedia sites, and for a limited time, it could be used to navigate to other sites, within a secure frame, and for a limited set of protocols, only HTTP sites; to vicite external HTTPS sites, the proxy will not be used, that proxy will cache these external visits in a Squid server, for a limited time : one hour max, isolating the sessions as much as possible, but this proxy won't support external cookies very well, except temporary session cookies so this may limit the interactions with these external sites).

  For the user's browser, all will appear as if they were visiting the randomized proxy as the main site, and the HTTPS session will appear being originating from of a visit of this WMF proxying site. Digicert won't be able to determine which Wikimedia project you're actually visiting with HTTPS connected to that random proxy (With SUL, the session is identified and communicated to other actual projects using internal security tokens, and a single session is established for all wikis. In fact the proxies are located directly on the existing farm of Squid servers for any WMF project. verdy_p (talk) 23:47, 20 June 2013 (UTC)

- **Comment** Why not making wkimedia domains availaible with the .onion extension in more than SSL. It would be a message that this extension is not only used by bandits. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 13:20, 3 July 2013 (UTC)

## Better supporting anonymous contributions [edit]

I repeat my comment: SSL or TLS ? And this is NOT off-topic, because you always use **SSL** when in fact you should speak about **HTTPS**.

> SSL is deprecated (and too much unsecure if we think about what developers PRISM can do) ! What I mean is that the level of security needed in HTTPS and supported by Wikimedia sites should be specified. The strongest algorithms should be used, and users should be warned if their connection configuration do not support it. Otherwise they will

feel **falsely protected** if they just see "https:" or the security icon in their address bar or status bar !

In other words, **Wikimedia sites should display the current security level of their connection. It should also allow evaluating the security of their local account** (user password, inspection of the email confirmation : users can copy-paste the MIME headers of the confirmation email they recieved, or the MIME headers of the last mail sent to Wikimedia for posting images, or the informations added in HTTP headers by some browser plugins, or inspection of their version and known defects, suggesting upgrades or removal of these unsecure plugins), even before they create a local account, or when creating it by evaluating the strength of their password, because the local account will be the only protection they'll have for their pricay, by hiding to others their connection IP.

If an account is stolen or spied (by an intruder that broke the security algorithms), it should still not allow inspecting the connection history. And may be it should even hide to users the email address that they have registered, by encypting it once the email has been confirmed (the only thing that a user will be able to do is to change the email address, or reconfirming what they think is their own address).

All registered users should be notified immediately at their old email address to confirm the change of email address (to avoid it to be replaced by another proxying and spying email address). As the email address will now be invisible in the user's preferences to the user as well as to any possible spier, it will be impossible to know who really owns that account (this should be kept by Wikimedia sites in a secure database (so all subscribed notifications will be sent to an address that no spier should know.

And Wikimedia should also monitor the security of its mailservers for its outgoing emails going to the email address of a registered user (this means securing its DNS server, asserting the DNS entries, using all possible antispoofind technics, verifying mail server secure signatures...), because these emails are the main tool by which a user could still be identified, even if they are IP-connected via an anonymizing proxy.

But of course, users that want to communicate with Wikimedia sites on *politically sensitive subjects*, should avoid revealing their own identity online in their talk pages or when discussing in any public spaces or on talk pages of other users.

Instead, they should create a new specific (and unrelated) account for these activities, using an alternate email for registering it. Then they should use tools offered in their User's preferences page to assert the securoty of this new account.

**Another idea:**

If users fear their account on Wikimedia has been compromized, they should immediately ask the deletion of this registered account, for possibly creating a new one (the contributions will be kept, but will be anonymized using a user name like "anonymous-<random-hexadecimal-id>" in the history, the old account will be locked and no longer accessible to anyone.

All users should be offered an oppotunity to create an "**publicly anonymous secondary account**" : if they have one, and make any contribution on Wikimedia using their normal non-anonymous account, then Wikimedia should ask them if they intended to use the anonymous account instead: they can confirm it each time or instruct Wikimedia to stop asking it for the next hour. If they want to use the secondary account, Wikimedia will present them a secure logon screen asking for the secondary password. As this account is anonymous, it should not need to be working under SUL (each wiki will use its own local database of anonymous user accounts). One they are connected to the two accounts, two icons are shown at top of page : their regular user name, and the "anonymous" account name, they can click on one of them to select which one to use (if they use the anonymous account, Wikimedia will not ask them to confirm their edits. If the anonymous session is idle for more than one hour, it will be automatically logged out (the session cookie should not last for more than one hour), and the anonymous icon will be shown in its disconnected state, even if they are still connected on their regular account (and Wikimedia will restart asking them if they want to use their anonymous account for their edits).

The secondary anonymous account may inherit immediately, at creation time, of some privileges from the primary regular account (notably the autoconfirmed status, but NOT any admin privileges). Users may also opt for creating an anonymous account directly, without any associated regular account (but then they'll start with no privileges, like all other newly registered regular users): in fact this should be the best solution for supporting anonymous users, we should encourage them to do so, instead of using their IP-only connection, logged in public histories (they can still register their email with it, and be sure that they'll be ale to reuse this same account on later connections): even if they are logged on, these anonymous users with a personal account should be kept logged on for a maximum of 1-hour of idle time (regular accounts may continue staying connected for 1 month). And even if they only have an anonymous account, they can also be offered the option to create a primary regular account, like other users (for their non-sensitive editing or reading sessions; in that case Wikmedia wil also ask them every hour if they should not use their existing anonymous account when accessing one page). Some pages should also not be warned by Wikimedia: the anonymous account may specify a ist of pages, or categories, or namespaces, where Wikiemdia will not ask them if they wish to use their anonymous account instead.

Registered anonymous users should also be allowed to participate to secured community polls (they will be able to vote only once), if this account is associated with a regular account (the vote will be visible to others as coming from a registered anonymous account, but then they won't be able to vote with their regular account as well). The secure vote server will check internally the status of the anonymous account, and will be able to see if the regular account has already participated or if another past anonymous account has voted (if so, users won't be able to vote again or will or change their vote, unless they ask to Wikimedia server to delete their old anonymous vote; this vote deletion will be performed securely).

Only one active (undeleted) anonymous account may be associated at any time to a regular account (this will limit abuses, notably with spammers, even if the CheckUser admin team may see with which regular account the anonymous account is associated. Some abusers may also be restricted (by spamfighters) from using their anonymous account for some time and informed. This event may be logged in their regular account that thay may continue to use).

This will also be useful when contributing in some subjects with the regular account, when there are personal conflicts (this could calm others, avoiding personal wars or personal defamation).

The list of past (deleted) anonymous accounts, as well as the current active anonymous account will be kept in the regular user account history, for a limited time, only to help fighting spammers; this should not exceed 1 month).

Creating and activating a publicly anonymous account should be a two click action (including for generating the password: users need to copy the generated strnig password, because it will later be encrypted and never shown again to anyone (including the user), but the user can request the deletion of this account and creation of a new one with a newly generatef password (overridable by the user typing a password of his choice and confirming it).

Even for regular (publicly non-anonymous) registered accounts, this should be simple, and Wikimedia should immediately propose a strong password before the user overrides it. All accounts (anonymous and non-anymous, should have a one-click button in their preference page, to generate a new string password and fill the two input boxes where they can change and confirm it (when the user types his own pawwsord, it is hidden by default, when the user clicks the "generate strong password", it will be shown and stay on screen, it will be used only if the user accepts it by confirming the preferences; but for accessibility reasons, there should still be a checkbox to hide/show the content of the password input and password confirmation box). verdy_p (talk) 23:29, 20 June 2013 (UTC)

## What types of logs does the Wikimedia Foundation keep, for how long and in what level of detail? [edit]

Before we can start to consider actions by the Foundation, I think it's appropriate for us to look at our own logs and how PRISM could affect us. There was a thread brought up on Wikimedia-l about this topic this week. I didn't have a chance to read it fully but from a brief skim of it, I believe it's unclear exactly what information the Foundation keeps, and for how long. There was a link to a mailing list post by Domas from 2010 saying it's a 1/1000 sample, but other comments referred to a full access log for the past 30 days. Therefore, please can we get the relevant technical details from **all** teams with access to logs of what data is stored and for how long? I don't know the full details, but a few ideas would include asking the Analytics team (who use the new Kraken machine), whoever is using the raw data to produce http://reportcard.wmflabs.org/, general reader access logs, error logs etc. **Thehelpfulone** 00:28, 15 June 2013 (UTC)

Yes please. We should assume any record we keep might be accessed one day so the best preparation for this is to minimise the records we keep. If we don't have them then they can't be accessed. Filceolaire (talk) 00:43, 15 June 2013 (UTC)

- Well, these are the things we know they have per browser operation and Help:CheckUser#Information returned; article accessed, date/time of access, referer, username, IP address, user agent (browser, operating system, blah, blah, blah) and XFF headers. Depending on who you talk to, this info is supposedly purged after 30, 60 or 90 days. But it has been acknowledged that some of this information is copied to the checkuser wiki, arb wiki, etc. where it is kept permanently. 64.40.54.96 05:35, 15 June 2013 (UTC)

> This shouldn't be a "depending on who you talk to" situation. We're pretty open about it - the data is purged after 90 days. Data on long-term abusers *may* be copied to the Checkuser wiki for later use in analysis to determine whether future vandalism is related to a long term abuser, but that's incredibly rare, when viewed as a percentage of the whole. Philippe (WMF) (talk) 07:53, 15 June 2013 (UTC)
>
> > I think the original comment was about access logs for readers, not authors who edit. For how long is the access log kept for readers and is there an access log for all readers or just a 1/1000 sample? --Tobias talk · contrib 08:00, 15 June 2013 (UTC)
> >
> > > I have no idea. Deferring to those who know. :) Philippe (WMF) (talk) 09:55, 15 June 2013 (UTC)

I second that question. A EU citizen myself, and even though Wikimedia might not own or borrow servers in the European Union, how close are the Wikimedia servers from the requirements of the EU law ? It was alleged here, in 2011 that *EU legislation, (...) requires search engines to purge all data relating to end users after a six month period*. User:Philippe (WMF) says above : "data is purged after 90 days". I am afraid that as long as this is not clearly written in http://wikimediafoundation.org/wiki/Privacy_policy , there is no guarantee that the Wikimedia Foundation is intending to enforce this kind of regulation and serious about it. Is there anything that can guarantee that the Wikimedia Foundation cannot change the present "90 days" of today into "90 years" tomorrow without warning and consultation with the community and sufficient warning of the end user as regards the "terms and conditions" ? Teofilo (talk) 18:49, 15 June 2013 (UTC)
Agreed: this should be part of our privacy policy. –SJ talk 23:48, 15 June 2013 (UTC)
I had always had the impression that logs of editing operations were kept around for a while, but access logs were not--and in particular that CU couldn't tell what articles people were reading. If they can, I find that scary and invasive, but potentially useful in sock investigations. I would urge getting rid of all logging of read-only accesses, including aggregated logging such as viewcounts on articles and geolocations. There could be some very limited exceptions for dealing with ops problems (DDOS origins, etc) but any such info (about human readers, I'm less concerned about automated clients especially malicious oens) should never be disclosed. 50.0.136.106 07:28, 21 June 2013 (UTC)

## Thirty day rule? [edit]

I thought there was some thirty day rule comment period related to proposals of this nature. Maybe I'm thinking of something else.

I suppose the Wikimedia Foundation could sign, but that wouldn't necessarily be representative of Wikimedia signing. --MZMcBride (talk) 00:55, 15 June 2013 (UTC)

> I assume you're talking about these policies? It doesn't look like there is a deadline (both a 'if times permits' clause to allow exceptions and no actual expectation of a deadline

spelled out) or do you mean something else? Jalexander (talk) 02:01, 15 June 2013 (UTC)

MZMcBride, that was for changes to the terms of use, I think. I'm not sure if the privacy policy is a subset of the terms of use, or if it's a separate contract. --NaBUru38 (talk) 20:21, 18 June 2013 (UTC)

## June 21 [edit]

What happens on June 21 that makes that day the final day of community consultations? Don't you think that it's at least eyebrow–raising that it took the WMF 8 days (since the news first broke out on June 6) to write a blog post, and you only give the community 7 days to comment on it? How are you planning to get the wider community to comment on this? Are there any plans for CentralNotice/Watchlist campaigns asking people to comment, or are you perhaps planning to use EdwardsBot to send a notice to the village pumps? odder (talk) 00:57, 15 June 2013 (UTC)

Hi, Odder - the blog post came out today, but we asked for comment on wikimedia-l and advocacy-advisors on June 11th (and have been following the conversation on both of those lists). That said, if the community thinks the correct answer is "take more time" we're open to that too; our main interest in speed is because the earlier we move, the greater the opportunity to actually impact the discussion. - LVilla (WMF) (talk) 01:59, 15 June 2013 (UTC)

Thanks for the explanation, Luis—I was mostly afraid that 7 days might not be enough time for the wider Wikimedia community to comment on this proposal. Your answer clears this up, so thanks again. odder (talk) 13:47, 15 June 2013 (UTC)

## Community Feedback [edit]

"It's important for Wikimedia to be a voice of opinion in these matters, but joining a group to back the opposition of PRISM doesn't seem like the most successful avenue to me. I think whenever an association is made with another organization or group of organizations it is easier for the whole group to find itself with potential liability. One company can never be completely sure of another company's origin, path and trajectory - take Invisible Children as an example - and the risk of being jointly discredited for something possibly inconsequential could affect the momentum of the movement at large. I think that many orangizations taking individual stances on the issue weighs heavier than a conglomerate doing the same."
—Glenn Sorrentino

Hi, Glenn- Many of the organizations behind stopwatching.us have extremely long track records of doing the right thing: EFF, FSF, and CDT have all been doing rights advocacy for around 20 years, and while Mozilla is relatively new to direct activism, it also has a long track record of having strong values like ours. That said, if you feel we should have a voice, just not through stopwatching.us, what other suggestions would you make about how we should advance our views? — LVilla (WMF) (talk) 16:11, 15 June 2013 (UTC)

Some might have a "long track record of doing the right thing" but some of their fellow

>> travelers are, shall we say, controversial. Snowden was photographed with an EFF sticker on his laptop, suggesting he supports these "strong values." Yet Snowden's particular version of what he presumably considers to be "strong values" led him to seek employment with his latest employer with the advance purpose of getting access to secrets that he could then reveal without authorization. This is controversial, to say the least. If it wasn't controversial, surely a country with a better track record on Internet freedom than China or Russia would be sheltering him. I am amazed at how the WMF keeps finding the bad guys in the form of large numbers of U.S. Congressmen as opposed to somewhere else (first with SOPA/PIPA and now with PRISM which Congress has long been aware of).--Brian Dell (talk) 17:29, 25 June 2013 (UTC)

## On establishing servers in other countries [edit]

At Meta:Babel#Wikimedia_servers_and_NSA_wiretapping I started a discussion on the possibility of the foundation establishing other servers in other countries partly so individual connections are less likely to be wiretapped.

Please read Stefan2's comments on that page.

So far Wikimedia has servers in Tampa, FL, Ashburn, VA, and Amsterdam. Considering that data usually takes the cheapest route rather than the most direct, where else should the foundation get servers? We have to take in consideration money that the WMF has and the political inclinations of the countries where the new Wikimedia servers are set up. For specific locations, would anyone like to evaluate the following locations? Singapore, Hong Kong, Brazil, South Africa... and I am not sure if the political climate in Dubai would support a WMF server there.

The idea is that, say, if an individual in Pakistan wants to connect to Wikimedia projects, he/she can connect to servers in Dubai, or if a person in Malaysia wants to connect, he/she can connect to servers in Singapore.

WhisperToMe (talk) 04:27, 15 June 2013 (UTC)

> I'm not an expert on this, but it seems to me that increasing the potential number of jurisdictions that servers live in actually increases the risk of wiretapping, not decreases it, right? I mean, any of those countries could order a wiretap on a server, and all of a sudden we're up from one potential governmental player to several. Philippe (WMF) (talk) 07:57, 15 June 2013 (UTC)

>> We have a server in the Netherlands, so that's two government players so far. WhisperToMe (talk) 14:38, 15 June 2013 (UTC)

>>> {{citation needed}}, please. odder (talk) 16:12, 15 June 2013 (UTC)

>>>> Wikimedia servers#Hosting says "As of June 2010, we have four colocation facilities:" with two in Tampa and two in the Netherlands, and "As of 2012 there are also servers in Ashburn, Virginia (eqiad)" WhisperToMe (talk) 17:11, 15 June 2013 (UTC)

>>>>> You wrote we had *a server* in the Netherlands, which is not true. Additionally, I would also suggest that you check what are the roles of the

NL servers before jumping to any conclusions. odder (talk) 17:16, 15 June 2013 (UTC)

Okay, so I should have said two servers or one location. Nonetheless the point was that we also have facilities in the Netherlands. Anyway I followed the link to "Server roles" on Wikitech from the Wikimedia servers#Hosting page, and the page is blank. However I found wikitech:Category:Servers (should I redirect "Server roles" to that page?). Each of those pages don't have information on geographical locations, but I found wikitech:Amsterdam cluster WhisperToMe (talk) 17:24, 15 June 2013 (UTC)

Doing further digging the Amsterdam cluster is a part of wikitech:Category:Esams cluster. I'm going to file through wikitech:Category:Clusters to get a count of geographical locations. WhisperToMe (talk) 17:30, 15 June 2013 (UTC)

Aside from the Esams cluster: wikitech:Category:Eqiad cluster -> Ashburn, VA. wikitech:Category:Knams cluster -> wikitech:Kennisnet cluster (Amsterdam). Lopar cluster seems to be in (Tampa) Florida (wikitech:Lopar cluster mentions caching out of Florida). Pmtpa cluster -> Tampa, Florida (wikitech:Tampa cluster). The page on the Ulsfo cluster (wikitech:Ulsfo) is blank. WhisperToMe (talk) 17:34, 15 June 2013 (UTC)

Okay, I found a page on the network design: Wikitech:Network design - It goes over the US network and the European network WhisperToMe (talk) 17:41, 15 June 2013 (UTC)

Notes some of the pages at wikitech are rather outdated. (For example, Isn't lopar long gone?). Perhaps looking through the lists of server types at ganglia would give you a better idea. My understanding [**which could be wrong**. Don't trust me. I do not know what I'm talking about] is that most of the "real" servers are in US, with esams (netherlands) having squid/varnish caching servers, that just forwards requests (other then anons who aren't editing) to the backend servers in ~~Vagina~~Virginia [Bad auto-spelling correct]. Bawolff (talk) 18:10, 15 June 2013 (UTC)

You mean Virginia, right? :) WhisperToMe (talk) 18:29, 15 June 2013 (UTC)

For our readers having multiple countries with servers may give some comfort, especially if there was some way to choose which server to connect to. I'm not convinced things work so well for editors, if you have more than one copy of a database open for editing you will get synchronisation issues. WereSpielChequers (talk) 14:56, 15 June 2013 (UTC)

That's a good point. Who are the WMF board members or officials who know the most about this? Based on the PRISM charts it may mean that Latin America & Caribbean and the Asia Pacific Regions may be the best place to establish Wikimedia servers (it seems like those in Africa can connect to European servers). So I think the WMF should study Hong Kong, Singapore, Brazil, and/or Panama (or another Central American country which can be neutral) as ideas for server locations. WhisperToMe (talk) 15:32, 15 June 2013 (UTC)

It is useless, according to the end of this film about the NSA wiretraping program (NSA - L'agence de l'Ombre) (author: James Bamford and C Scott Willis) (2008), the NSA is also watching all strategic point of internet accross the world, with subprograms affilieted indirectly to PRISM. So it is not limited to the US. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 21:40, 15 June 2013 (UTC)

Does the film say where these end points are? WhisperToMe (talk) 00:17, 16 June 2013 (UTC)

No, they don't list all of them.The film say there are sattelite communication sniffing. I can also say that certain under sea cable landing have optical splittering circuits. The film give only details (to show an example) about Moro Bay in California: It give a full explaination about where the data is collected. You can find some part of the example at cryptome, but you won't understand many things with this web page.
The film is based on a book : The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America.
You have a lot of more information on those parts with the film rather than the PRISM leaks.
The orignal language is in english, but as I saw the film on the TV, all was translated, including the title. I can't find the original one.
2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 03:10, 16 June 2013 (UTC)

Thank you for the info! I'm going to try to find this book and get as much information about NSA wiretapping locations (now we will assume whatever Bamford says is true) as possible and perhaps the WMF can find information on how best to avoid this wiretapping. Locations for new WMF servers can be based on this information. Also it may be good to have backup servers in "neutral" countries in case the possibility of war comes. I would hate to see all of our hard work wiped out. I have been working on Wikimedia projects for almost ten years, so I'm sure you understand how I feel about this. WhisperToMe (talk) 02:56, 17 June 2013 (UTC)

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA: I saw a video on YouTube which seems to be what you watched.

- Bamford's message was routed from en:Kuala Lumpur, to en:Mersing, Malaysia where it entered an undersea cable along the South China Sea to through en:Shantou, China, and then in an undersea cable to an area near en:Morro Bay, California, to a building near en:San Luis Obispo (80% of all communications from Asia to the US enter through this building, but under new NSA orders they don't tap in here), and then to the AT&T Regional Switching Center in en:San Francisco (this is where the NSA taps into the connection) -- So, if I am correct, if the reader traffic in East/Southeast Asia goes to Singapore or Hong Kong and it doesn't go via satellite, it will avoid

the NSA tap in San Francisco
I'll check if the NSA book has more information
WhisperToMe (talk) 06:10, 17 June 2013 (UTC)

I won't have a static ip this week. If you want to know which routers is used by a request, I suggest you the **tracepath6(article)** command. tracepath give you generally more details (more hops) than traceroute. Here is an example of a traceroute6 result from Dalas:

```
hop     rtt     rtt     rtt       ip address           fully
qualified domain name
1       7       7       6         2001:470:1f0e:513::1
hexillion-2.tunnel.tserv8.dal1.ipv6.he.net
2       8       1       1         2001:470:0:78::1     gige-g2-
14.core1.dal1.he.net
3       29      25      24        2001:470:0:1b6::2
10gigabitethernet5-4.core1.atl1.he.net
4       33      41      34        2001:470:0:1b5::1
10gigabitethernet16-5.core1.ash1.he.net
5       39      38      58        2001:470:0:299::2
100gigabitethernet7-1.core1.nyc4.he.net
6       108     107     116       2001:470:0:128::2
10gigabitethernet1-2.core1.lon1.he.net
7       118     115     138       2001:470:0:3f::21
10gigabitethernet1-1.core1.ams1.he.net
8       117     117     117       2001:7f8:1::a504:8539:1
9       120     125     124       2a00:d10:1144:61::468
vlan61.br.en1.oxilion.net
10      121     121     121       2a00:d10:1144:62::731
vlan62.n5k-a.en1.oxilion.net
11      116     116     116       2a00:d10:101::11:1
ergens.org
```

```
dal=Dalas
atl=Atlas
I don't know for ash
nyc=New York City
lon=London
ams=Amsterdam
```

If you want a good answer for server location: The best place for data center is everywhere in the world.

Let me explain: There is a technique originally created to reduce load on the public network. Instead of creating a big server in one place (wikmedia use also separate severs in Europe), you choose to have "medium" data centers divided all over the world. Each place contain a copy of the whole webs sites. With a same host name, the list of ip address you get will varies according to servers workload and your geographic location.

This technique of geographical web placement has a name,(which I forgot) and probably a wikipedia article. It is used by big firms like Google. You can make the test on companies like these: If you launch a tracepath, the number hops will be always fewer than most sites, and independently from the place you are located.

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 02:19, 18 June 2013 (UTC)

> I'm in the US myself, but this would be fun to try! According to your vision, do you have cities in mind which would be good places for these medium data servers? How many such medium servers would you establish per continent? WhisperToMe (talk) 05:27, 18 June 2013 (UTC)
>
>> Sorry, I've been busy since last time. I'm afraid that I don't have a real answer. This is just something I learned when I was studying DNS. I know google have serveral location in europe, but if I do a host on yahoo...

```
root@sysresccd /root % host www.yahoo.com
www.yahoo.com is an alias for fd-fp3.wg1.b.yahoo.com.
fd-fp3.wg1.b.yahoo.com is an alias for ds-fp3.wg1.b.yahoo.com.
ds-fp3.wg1.b.yahoo.com is an alias for ds-eu-fp3-
lfb.wa1.b.yahoo.com.
ds-eu-fp3-lfb.wa1.b.yahoo.com is an alias for ds-eu-
fp3.wa1.b.yahoo.com.
ds-eu-fp3.wa1.b.yahoo.com has address 87.248.112.181
ds-eu-fp3.wa1.b.yahoo.com has address 87.248.122.122
ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
2a00:1288:f00e:1fe::3000
ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
2a00:1288:f00e:1fe::3001
ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
2a00:1288:f006:1fe::3001
ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
2a00:1288:f006:1fe::3000
```

>> there are alias which contains eu. It make think yahoo have only one point for the whole european union. You probably won't have the same density in south corea as in Sahara. I must say that I know absolutely nothing about the synchronisation thecniques that are used, and i don't realy know sor dns too.
>> With the high number of law voted in US & eu for alowing thing this, I don't understand why peoples warm only now. If you think to the number of contries where drones work. You can realize most of peoples are safe.
>> For the rest of the world the main risk is unemployment, but it is not linked to any government. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 14:08, 3 July 2013 (UTC)

## Should we join with these organizations in their public statements and efforts as they relate to the Wikimedia community's values and mission? [edit]

- Yes, please. --Kellerkind (talk) 08:36, 15 June 2013 (UTC) (Hello, NSA!)
  - +1 --Isderion (talk) 13:54, 15 June 2013 (UTC)
- Should Wikimedia join in decrying PRISM? No.

  It was OK when Wikimedia decided to make a stand on SOPA, b/c SOPA legislation had clear and obvious detrimental consequences on the functioning of Wikimedia.

  It is not clear or obvious how PRISM or FISA has negative consequences on Wikimedia. In my view, the Foundation seems to have adopted the role of an internet freedom fighter, wanting to take a stand against anything perceived to threaten web users' privacy and freedoms. Now, that might be an admirable position, but it's also to some extent a political position and one that clashes with the foundation's longstanding principle of remaining neutral on such issues. moved from blog, comment by Nicholas Sammons : 2013/06/14 at 7:59 UTC by Jalexander (talk) 10:11, 15 June 2013 (UTC)

  > To be neutral about the knowledge inside Wikipedia and being neutral about the way internet works are not the same thing. If we want a neutral point of view inside Wikipedia, we need to protect free use of internet for dissident opinions to be able to exist. I think the Wikimedia Foundation should fight for the freedom of internet. Lionel Allorge (talk) 11:03, 15 June 2013 (UTC)

  Staying neutral in the face of a global wiretapping action by the US isn't neutral. Silence means saying "Yes" to this actions. We shouldn't do that. It is pretty clear how Wikimedia is affected by PRISM. It is about trust in internet use at all which then includes the never to be answered question about the tracking of your own search habits on Wikimedia projects.
  So I vote Yes for at least joining the public statements and efforts according to the role Wikimedia can do relating to its community's value and mission. --Jensbest (talk) 13:26, 15 June 2013 (UTC)

  > Then I guess we would all appreciate if you let us know *how exactly* Wikimedia is affected by PRISM and how is it involved in the scandal that broke around it if you think it's *pretty clear*. For me it isn't, so I would welcome an explanation. odder (talk) 13:46, 15 June 2013 (UTC)
  >
  >> You can't look on Wikimedia without reflecting on its digital environment. If the web as a whole is monitored by a state, Wikimedia, with Wikipedia being one of the biggest websites in this web, must take a stand according to its values and long-term practices. It isn't about the question if there is any Wikimedia-Staff forced to lie to us because of secret judge rulings and gag orders, it is about the fundamental question if there can be a free, not-state-monitored encyclopedia in a non-free, state-monitored web. The actions of the US-government spreading massive distrust all over the web. Distrust is endangering the emanzipatory and participatory culture of the web which is also an important foundation of all Wikimedia-projects. --Jensbest (talk) 18:28, 15 June 2013 (UTC)
  >>
  >>> Certainly Wikimedia does not have to do anything. It is the Foundation's (or rather the community's) choice whether to take any action, which is precisely what is being debated here. There is no information whether any

government monitors the whole web, PRISM is only about one government monitoring services of a couple of companies (however big they are). However, it's common knowledge that the Web, or some parts of it, has been monitored and censored for a long time (take China, Qatar, Egypt, Syria, and now Turkey as examples), and the Wikimedia movement did not protest against that. odder (talk) 18:57, 15 June 2013 (UTC)

Certainly Wikimedia has to do something when the country in which most of its servers are hosted is convicted doing massive secret global webwide monitoring. You are wrong on how PRISM works. It is sweeping the web at a whole AND is using direct access to thousands of companies. Therefore my point made above is very relevant - there is no good web use inside a corrupted system, there is no free and anonymous use when the leading country of the so-called free webworld is doing massive global secret surveillance. The other "argument" that the web is partially state-monitored anyway and therefore any action would be useless is definitely the most fatalistic and irresponsible opinion on freedom I've heard for a long time. --Jensbest (talk) 20:52, 15 June 2013 (UTC)

How do you know that? As far as the media report the situation, PRISM is related to a small number of Internet service providers, if you take the global picture into consideration. Plus, I've never said that Wikimedia shouldn't act — I only said that it *did* not act when there were reports on how Chinese, Syrian, Egyptian and now Turkish governments monitored and censored the Web. We have millions of readers in those countries, and yet there wasn't any suggestion for the WMF to join the local initiatives for a free and unmonitored Internet — if we're acting now, then I'd think it be just fair for the WMF to react whenever there are reports on monitoring Internet users in countries reached by our projects. odder (talk) 21:09, 15 June 2013 (UTC)

I agree with you that it is a question of how to balance decisions on taking action. Maybe Wikimedia should have a more fundamental permanent stance on the subject, but being based on the idea of openness and collaboration Wikimedia has to stick to the more complicated and sometimes tedious decision-finding process by asking the community. This doesn't make us as effective and "punchy" as other digital NGOs more focused on fighting for digital rights like EFF etc. - But then again, if this "big ship" Wikimedia is moving it means something for more people even beyond the digital filterbubble. - According to your question about the broadness and depth of Prism and related state-surveillance activities I don't wanna spam you with articles, so just one for some sunday lecture: a longer overview-article by AP. --Jensbest (talk) 22:23, 15 June 2013 (UTC) one potential argument: Wikimedia relies on editors being able to edit freely without real world retalation. This is one reason things like no legal threats is a policy. If editors fear retalation by gov for the things they do on wikimedia, they wont do things that might piss off gov. Amount of systemic bias in Wikimedia could sky rocket. Obviously we arent at full survalience/police state yet, but things like that happen one small step at a time. This is a large step. Bawolff (talk) 15:17, 15 June 2013 (UTC)

- Yes we should decry PRISM, unless that is the US government announces that it wasn't monitoring Wikimedia traffic. If they give an assurance that they weren't snooping on us then Wikimedia should revert to neutrality as that would be consistent with only reacting to direct threats. Decrying is much less drastic an action than a blackout, and I think that it would be an appropriate level of action. WereSpielChequers (talk) 15:01, 15 June 2013 (UTC)
- That's definitely compliant with Wikimedian values and long-term practices: Wiki contributions are based on the premise that we are not forced to disclose our *real* identity. Alexander Doria (talk) 16:07, 15 June 2013 (UTC)
- I applaud the Wikimedia foundation for taking action.

  It is to my knowledge that the “collection” of data from those internet companies mentioned in the leaks are not done willingly, but unknowingly through a massive collection of packets that travel to and from their data centers (very similar to the upstream method found here http://en.wikipedia.org/wiki/Room_641A).

  If this is true, the only preventative way of circumventing such “prism” taps would entail allocating your data centers, specifically for North America, outside of United States jurisdiction — to Canada and Mexico, for example. However, user packets that are sent to and from Wikipedia are still very vulnerable as they will traverse private ISPs in the U.S., those of which are supposedly already under surveillance.

  An immediate response would be implementing a secure SSL connection for users inside the United States.

  I hope the Wikimedia foundation, along with other key organizations, continue to fight for a free, open and secure internet.

  I thank you all for your efforts. moved from blog, comment by Mark B : 2013/06/15 at 21:47 UTC by Jalexander (talk) 01:07, 16 June 2013 (UTC)
- Yes, the WMF should join with these organizations and support efforts to protect internet privacy from warrant-less removal. - Amgine/meta wikt wnews blog wmf-blog goog news 16:35, 16 June 2013 (UTC)
- ⊕ **Support** – We should stand with the Internet and against government spying. --Michaeldsuarez (talk) 23:11, 17 June 2013 (UTC)
- The WMF board should feel free to make a statement, if there is consensus for one, and individual board members should feel free to campaign as individuals as much as they wish, but I would be firmly opposed to a PRISM blackout in the style of the SOPA blackout. While I understand the temptation to wield political power, the project as a whole should not be a political actor, but remain neutral. Andreas JN466 10:32, 18 June

2013 (UTC)

- **Oppose** Per Andreas. --Anthonyhcole (talk) 12:37, 18 June 2013 (UTC)
- **Oppose** - I believe it's already been acknowledged by the Feds that to the extent that info is being collected beyond that pursuant to a particularized request, it's because they are data mining and data mining more or less by definition means the queries are not particularized. I don't think people fully understand just how different this is from prying eyes reading your personal email. On the other hand, were the WMF to gain media attention for its activism here, in my view it would provide some evidence for my claims at the the time of the SOPA/PIPA activism that the WMF feels compelled to weigh in on civil liberties issues that are of dubious if any connection to the development of Wikimania projects.--Brian Dell (talk) 18:44, 19 June 2013 (UTC)
- **Comment**. WMF needs to find out, in detail, whether any of these programs **potentially** affect Wikipedia, which is a different question from whether information has been delivered so far. My assumption is that potentially yes, they could be served up a NSL tomorrow demanding data on everybody who reads w:Acetone peroxide, etc. Indeed, it seems too tempting a resource for me to be entirely credulous that the NSA has passed it up so far - surely there were a few days a while back when they would have wanted every possible means to know who looked up anything about pressure cooker bombs from an IP address in Boston. In opposing this, we oppose what seems like a very sensible police tactic, and we have to do so on the basis of weighing the mild harm against the vast multitude against the chance of preventing grievous harm to a few - and in an age of locking down a whole city, there are clearly some authorities making the wrong decisions about things like that. We'll need more transparency about how search warrants/subpoenas for such things are *legally* delivered, and what protections there are there. What we need here isn't a vague feeling, but a well-constructed ideological fortress. We just need a lot better data and thought about all the issues involved. It is unfortunately likely that, far from being on the offensive, Wikipedia will find itself trying to argue against *mandated* data retention policies that have been promulgated in many contexts, trying to preserve what it has now. Wnt (talk) 21:48, 19 June 2013 (UTC)
- **Support** Prism (according to some people) presumptively examines all Wikipedia traffic (along with all other internet traffic) from Room 641A and similar locations. Therefore its operators monitor everything everyone is reading (even if only metadata is logged, that is enough to deduce the content being read, from message sizes). This has potentially major consequences for readers and therefore is a matter of serious concern for Wikipedia. Even if the allegations turn out to be false, they are plausible enough to have a chilling effect in their own right, so Wikipedia should intervene either way. I personally support major changes in Wikipedia operations and practices to deal with this, but that's beyond the scope of this immediate question. 50.0.136.106 07:14, 20 June 2013 (UTC)
- **Support**. I don't fear US where I'm located in France. Though I still fear blanket cooperation of France with US to provide everything that US requests. But I would need to violate French laws. I don't fear the consequences of my opinion and I'm free for reading everything I want. But I stil think that users around us are in severe troubles, and US action will create a precedent that will be followed by other countries (notably in

China, and in all Islamic countries, as well as Russia, against their political opponents; LGBT people for example are in severe troubles now almost everywhere in Africa, Russia, Central and Southern Asia, Indonesia, only by the fact they may read about these topics or give their opinion, or present the facts about what happens in their country, or translate articles about their country originating from foreign countries into their national language : this is even more critical for languages that are not major, like Azeri, Uzbek, Burmese, Persian, Urdu, Indonesian/Malaysian, Javanese... and most African languages, because there's not a very active and protected community abroad using these languages on Wikimedia projects... If people in these countries cannot read major foreign languages, they will be presented a skewed view. This view will be skewed (NPOV) even in Wikimedia sites edited mostly by other national residents of their country). verdy_p (talk) 00:26, 21 June 2013 (UTC)

## Update [edit]

Hello all, thank you to everyone who shared their feedback above. Based on this consultation, there is limited support for advocacy about government surveillance, such as PRISM. We are currently evaluating possible advocacy options that are consistent with this feedback. Particularly, we are looking for options that are focused on government surveillance from an international perspective. You are welcome to continue to leave feedback and suggestions, and I will keep you updated. Thanks again, Stephen LaPorte (WMF) (talk) 18:52, 5 July 2013 (UTC)

15 threads, 10 support, 1 comment, 4 oppose (66.7%, 6.7%, 26.7%) - Amgine/meta wikt wnews blog wmf-blog goog news 17:28, 8 July 2013 (UTC)

But also a fair amount of negative feedback in other parts of the discussion (e.g., "US Issue" below, some of the blog comments), so my sense is that a pure count of the (very small) numbers does not mean much. Honestly open to persuasion/discussion on that point, though. LVilla (WMF) (talk) 17:39, 8 July 2013 (UTC)

Actually, I took the liberty of examining the remainder of this page. Not one thread did I find which stated opposition to action on this topic. There were questions about whether this is a a solely US topic (which, in a manner of speaking, it is, as it's the US NSA whose actions are being discussed.) There were discussions which suggested this is diversionary. But none opposed acting on it. Perhaps you're referring to discussions elsewhere and ascribing them locally as none expressed opposition to acting on this topic as far as I could discern. - Amgine/meta wikt wnews blog wmf-blog goog news 07:03, 9 July 2013 (UTC)

If we feel that "stopwatching.us" is too US-centric, I think it would be appropriate for us to post a similar statement of our own, framed more globally:

- Indicating that we will support regional or national efforts to keep this aspect of the web open, because of its impact on the free exchange of knowledge.
- Listing the national/regional initiatives we are aware of, which we may or may not have expressly signed on to.
- Listing and amplifying the participation of Chapters and other regional Wikimedia groups who have supported those regional initiatives.

- Encouraging the global Wikimedia community to help keep the Web open in this fashion.

–SJ talk 18:34, 8 July 2013 (UTC)

## Stop logging IP addresses [edit]

Currently and as far as I'm aware for the life of the project, edits by IPs have been publicly and permanently logged by full IP address on our databases. For me as a Brit that has never been an issue, and I even linked a couple of IP addresses I'd used in one of my RFAs. But to others it is an ongoing issue, I gather that much of our oversighting relates to accidentally disclosed IPs. IPs present a real security risk, for example an IP editor in a totalitarian country might not be aware of what irritates the regime, might be unaware that their IP is so easily tracked to them, might be caught out by an unexpected change of regime or may simply lose their temper and say something that puts them in trouble. We could fairly easily reduce these risks this by assigning temporary codes to IPs that edit. Unless there were a block in place, the codes could be reset every few months. Checkusers would still be able to look at recent full IP addresses. Other editors could still see which other edits had been made by the same IP during a period of months. But once the codes changed even the checkusers would only be able to link the IP addresses of last few months edits to defunct temporary codes, much as is the situation with logged in editors. Arguably the US would be the Government least affected by this security measure. But a boost to the security of an oft neglected part of our community would be a reassuring response to PRISM. WereSpielChequers (talk) 15:41, 15 June 2013 (UTC)

> Stopping logging IP's will be a problem for the fight against spammers. But a solution is would be to transfer all logs outside US in a safe haven, in compressed batches, leaving just the minimum logs needed for performance, on a short timeframe.
>
> However the US law may still already require that service providers keep a minium amount of logs for inspection. In all cases, these logs must be severely restricted from random accesses, kept on servers in encrypted forms. And most probably, there should no longer be any user with CheckUser capability ni US or acting under US law.
>
> Note that many other countries already have such laws requiring keeping a minimum amount of logs for judiciary requests. In some countries this could be just a couple of months, in some others the requirements may extend to several years. For very visited sites, this means a cost not only for the storage, but also to ensure that it will be correctly backed up and saved from severe crashes, so that they remain readable (this implies additional maintenance costs for these backups, possibly offsite, or could require transfering these logs to a legally approved legal escrow, that will also want to be paid for this service... or directly to a governmental department).
>
> For now the WMF is locating most of its servers in Florida and has to comply to the laws of US and Florida (some servers for tools or for proxies are also located in Europe : proxies also may need to keep these connection logs.
>
> In some countries, users already can only to Wikimedia sites by using mandatory national proxies). Most users accessing to WMF sites via mobile Internet accesses are also using proxies maintained by their ISP, which will keep these logs (in addition to restricting the protocols, for example only HTTP, or HTTPS only for authentification and

data signatures for securing commercial/bank transactions, but not strong encryption!).
But the scope of PRISM is not just about connection logs to help tracking network paths and identify the senders. It is really in inspecting the contents sent, and getting access to the full user profiles maintained by websites (for example the full list of emails sent and received with their content and metadata, and precisce timing of user interactions with any online service : this includes the Internet, as well as GSM networks or any other electronic transport path).
The solution would be transmit data hidden within analog signals or strong random noise fields with steganographic technics (those that are used by militaries that can hide their transmission within the mediums used by regular commercial channels, by slightly modifying it in an invisible way (a way that does not break the existing protocols, or that just generates a small amount of random errors that these networks tolerate.) But Wikimedia is not a military organization, and these technics are very costly (they constantly need to be adapted, this implies huge unamortized development costs). verdy_p (talk) 16:29, 15 June 2013 (UTC)

> Note, one has to be careful when designing such a system, as it is shockingly easy to design something like that poorly, and have it be no more private then just putting the IPs of anons everywhere. Historically, if you go back far enough (aka during phase 1 time), we actually blanked out the last 3 digits of the IP address so it was just xxx. (AFAIK we stopped because this didn't actually provide any "real" privacy). A second problem is that each IP address is not an independent number, they are related. If we replaced each IP with some sort of hash of the IP, we wouldn't be able to as effectively investigate vandalism that comes from different IPs from the same network. Range blocks also would be a thing of the past. Bawolff (talk) 18:16, 15 June 2013 (UTC)
>
>> Good points, yes a careful redesign would be needed, and we still need to retain the ability to rangeblock. I think it is time for a major review of this area, both for privacy and to reduce collateral damage. For example range blocks are notorious for effecting lots of innocent parties, *smart rangeblocks* would only block edits by people with the same hardware and and browser configuration as the problematic editor. WereSpielChequers (talk) 23:55, 15 June 2013 (UTC)
>>
>>> I'm inclined to agree with WSC about this, but honestly -- I always assumed the reason why Wikipedia lists the IP addresses openly was to spare government agents the trouble of coming in and requesting them (and themselves the trouble of giving them out). Wikipedia's structure has in many ways seemed like a reaction to long-term spying, where so little is kept that is *not* public that the spies barely have an advantage over anybody else, which may be the best anyone can achieve now. Wnt (talk) 21:51, 19 June 2013 (UTC)
>>>
>>>> We have no longterm need for most IP data, and the spies can't request what no longer exists. OK there are some scenarios where this would be of little use, but what about where governments change and a new government wants to know things that one could have trusted the old government not to ask? WereSpielChequers (talk) 12:13, 30 June 2013

(UTC)

## "law-enforcement agency or a court or equivalent government body" [edit]

http://wikimediafoundation.org/wiki/Privacy_policy uses "law-enforcement agency or a court or equivalent government body" language. Does that include the en:National Security Agency ? Teofilo (talk) 18:56, 15 June 2013 (UTC)

## A U.S. issue? [edit]

The fact that WMF is concerned about privacy-eroding actions by the U.S. government is commendable, and I completely agree with ALA's statement quoted in the blog post: "rights of privacy are necessary for intellectual freedom". I also agree with the statement that "the global nature of internet traffic, and the alleged sharing of surveillance information between governments, means that Internet users around the world are potentially affected". However, as far as the issue has been handled by the organisations in the *StopWatchingUs* coalition up to now, the matter falsely seems to be only affecting U.S. citizens. We, non-U.S. citizens, have been ever treated as second-class humans in U.S. law: the safeguards against illegal wiretapping in FISA and PATRIOT act only apply to U.S. citizens. And despite the fact that the alleged surveillance potentially affects hundreds of millions of people around the world, the *StopWatchingUs* coalition is calling to "*Enact reform this Congress to Section 215 of the USA PATRIOT Act, the state secrets privilege, and the FISA Amendments Act to make clear that blanket surveillance of the Internet activity and phone records of any person residing in the U.S. is prohibited by law and that violations can be reviewed in adversarial proceedings before a public court*". That would surely be a good step forward for U.S. citizens, but still leaves out in the cold us. By "us", I mean the people *from abroad the U.S.* that access the Internet *from abroad the U.S.* to send contents to or retrieve them from *abroad the U.S.* and whose packets are routed through the U.S. (as 60 % of Internet traffic does). If WMF intends to push a less U.S.-centric approach in this issue, please count with all my support. But, please (and perhaps once in a lifetime), please stop seeing U.S. as the very center of the Universe. Thanks, Cinabrium (talk) 23:10, 15 June 2013 (UTC)

Blanket surveillance of the use of US servers is a global issue. The language of this page does not suggest otherwise. We should focus on the underlying principles of privacy, which are universal. –SJ talk 23:48, 15 June 2013 (UTC)

@Sj But the letter by StopWatchingUs does *not* focus on “underlying principles” but on some aspects of US law only affecting US citizens. That was Cinabrium’s point. --Chricho (talk) 01:15, 16 June 2013 (UTC)

Exactly. Thanks, Chricho. Wikimedia projects house a huge international community, which is affected by U.S. surveillance policies (and in a non trivial number of cases, by those of their home countries too). If WMF's actions on this issue will be limited to endorse the *StopWatchingUs* letter, then nothing would have changed for those member of the community out of the U.S. Furthermore, while demanding transparency and respect for privacy from the U.S. government, and taking into consideration the transnational nature of the community, WMF should engage in similar actions wherever privacy and freedom of expression are harmed by sevretive laws and Star Chamber procedures. Canada, Sweden, Italy and India are just examples of legal frameworks allowing forms of surveillance even more invasive that those in the U.S. I'm not opposing actions with regard to NSA's PRISM scandal (I would add BLARNEY, NUCLEON, and many other questionable systems). I'm just saying that WMF's actions should be directed to protect some fundamental rights of the whole Wikimedia community, wherever those rights may be at risk. Cinabrium (talk) 08:56, 16 June 2013 (UTC)

> Hello, Alex Fowler here from Mozilla, one of the sponsoring organizations behind the StopWatching.Us campaign. We are also a community made up of thousands of contributors from around the world. Starting this week, we've broadened the campaign site to be inclusive of citizens outside of the US. More is underway to broaden input and dialogue from around the world. We'd benefit greatly from this community's participation and ideas on other ways to globalize campaign messages and actions.
>
> > Hello, Alex! Endorsing this statement (and convincing other organizations to do the same) could be a good starting point for globalizing the campaign. Cinabrium (talk) 17:38, 19 June 2013 (UTC)

I agree with Cinabrium's and Chricho's remarks. --NaBUru38 (talk) 20:34, 18 June 2013 (UTC)

## Comments copied from Blog [edit]

- The united states government is only trolling the very low hanging fruit. Any serious netherios group knows the ways to circumvent detection. Its reminiscent of "weapons of mass destruction" and will be lapped up by the chattering classes on the net. Anonymous. Copied from blog; Comment by Anonymous 2013/06/15 at 00:37 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)
- What people want to know is this:
  "When I read Wikipedia is the government reading over my shoulder, logging my activity, and potentially inferring my politics and values?"

  But they cannot find the answer to this simple question in your post. Allow me to help you with a frank answer:

  For some users the answer is unequivocally yes: Wikimedia has _specific_ knowledge of authorities in some countries intercepting and monitoring traffic to Wikipedia.

  For users who are concerned about observation by the US government the frank answer is "We probably couldn't tell you if it were so, so asking us is pointless."— if Wikimedia was ordered to lie by the United States government it would lie. It might fight such an order but it would lie until it won. Furthermore, individual members Wikimedia staff may also be acting under the influence of the US or other government without Wikimedia's knowledge. It is difficult to be sure of the absence of surveillance.

  Wikimedia also currently keeps detailed access logs which may be subpoenad (or stolen) at some time in the future and used to look for people (by IP address) were reading particular articles or which articles a particular IP address has read. Similar data— in the form of search engine logs— has been used in US courts in the past to prosecute people.

Fortunately the readers of Wikipedia aren't helpless and don't have to trade privacy for knowledge:

- If you use the https-everywhere browser add-on (https://www.eff.org/https-everywhere) the identify of the specific articles you read are hidden from any party who does not have Wikimedia's cooperation.
- If you browse using Tor (https://www.torproject.org/) then your Wikipedia reading habits will be kept more private even if Wikimedia is cooperating with parties conducting surveillance, and the fact that you are using Wikipedia at all will be hidden.
- For smaller Wikipedia languages it is feasible to download the entire Wikipedia and read it offline at your leisure (http://en.wikipedia.org/wiki/Wikipedia:Database_download)

You can also limit your Wikipedia browsing to public wifi networks, although many keep logs, and libraries systems where no identification is required.

These actions can keep your reading private regardless of the specific surveillance program of concern or Wikimedia's level of (non)-participation. Copied from blog; Comment by Greg Maxwell 2013/06/15 at 01:21 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)

- The US government doesn't believe in humans, their values. So the PRISM happened. Copied from blog; Comment by arun 2013/06/15 at 03:59 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)
- About note 2: it has been revealed that the alleged minor limits on the scope of surveillance only applies to US nationals living in US, but in fact this is only determined by a fuzzy reasonnable conviction that the location and nationality Internet user is not really very well determined. These fuzzy limits imply that more than half of US citizens will be spiable independantly of these limits.
  The limitations of budgets for the US agency means that they will in fact just scope some keywords to determine this.

  In addition this minor limitation of sope also means that US citizens located abroad, or accessing the Internet via foreign networks will be spied without knowing it. As well, the world trafic from abroad that can reach a US network is tremendous, due to the many third-parties involved in delivering Internet services in the world. So anyone in the world will not be subject to these limitation of scope, and can have their personal data or opinion gathered, stored, and searched in the US agency "Big Data" systems, and kept for unlimited time.

  There's absoutely no limits on the usage that will be done about these data, and it may be used to exercise pressures against people around the world, only for their political, social or economical views or actions, even if these actions are perfectly legal in these countries (and rules there by laws protecting their privacy). This could then be used not just for fighting against terrorism or international criminality (this is already allowed within international cooperations of law enforcement polices, under the scrutiny of national justice systems), but for any concern that the US government judges will be useful to protect its own economical interests, such as limiting the capability of saling things to US, or threatening them of nex taxes, or harassing their contacts in US that still work there in full compliance with US laws (for example refusing to contract with them, without having to justify why).

We've already seen people denied access to US when boarding a plane or only when they put their first foot on a US airport, for many false (unverified) allegations of links with terrorists, or international criminals, or their providers, only because they had a name similar to a growing list of people created in a multi-level web where those people have never had any contact or nay reason to believe that they were in contact with these seeked people. Every month now, this costs a lot of money to travel agencies around the world (or in US), and people are held in custody temporarily and ejected back to their country, based on false allegations or suspiscions. And legal contracts are broken unilaterally by the US governement? All these actions are made without any compensation (people may only defend their case in a US court, but they cannot go there and the only mean for them would be to pay a very costly US attorney, acting alone with very limited informations collected : only rich people can pay these services, without any warranty that false allegations or suspiscions will be removed from the databases, and new difficulties will reappear later, even if the initial allegations were proven completely wrong).

On the opposite, the US in fact does not collaborate with the same scale to fight against some US criminals, and offers a passive protection in many cases, not really limiting their actions (notably in cases of financial abuses and Internet abuses).

It is wellknown that US even pays them to act abroad, and will protect them by offering them immediate asylum in US in case of problems, and that legal threats against them abroad will be alerted to them, to limit the legal actions or embarass the investigators (using private information collected illegally from them, without them having any action in US, or against US, or being aware that this may impact some US politics or interests, other than fair and legal competition protected by international treaties and conventions).

This system of Internet surveillance is very unbalanced when we measure how the Internet is controlled from US, or its services are hosted in US for most critical operations, as well as a broad cloud of third-part providers of services (and of proprietary softwares, hardwares and very important technologies such as encryption, DRM systems, the PKI… and even HTTPS itself). The US detains the power-off button to cut any one at any moment from most parts of the Internet (even on services made abroad and not intended really to be used in US). The core infrastructure of the Internet cannot work without US control (or it can only work in a very limited subnetwork, but not on the "open" Internet we use everyday via our foreign ISPs, that are often liable themselves in US where they have some subsidiaries, and via international stock markets controling their corporate governance).

For these reasons, your note #2 tends to reduce the severity of the effective impact of

> this surveillance. Probably only about 100 millions of US citizens will be protected, within a world of 7 billions people (this is about 98.5% of the world population that will be under possible US scrutiny of their legal private life, at any time and for no reason at all at the time of this surveillance, but who will become some years laters to difficulties or personnal harassment…) Moved from blog comment by Verdy_p on 2013/06/15 at 09:45 (UTC) by Jalexander (talk) 01:20, 16 June 2013 (UTC)

## PRISM concerns Trust, Trust concerns Wikipedia [edit]

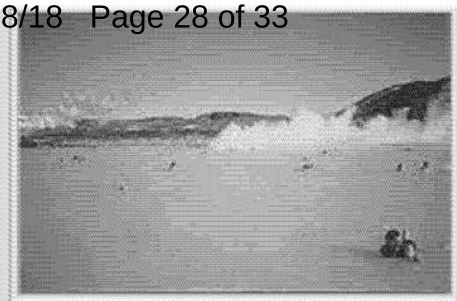
I strongly support any steps by the Wikimedia movement (including WMF) to openly oppose PRISM and similar spy programs. Though currently there is little certainty about what exactly is happening, it is clear to me that NSA spying has the *potential* to violate privacy rights of our users on a massive scale. As a main source for unbiased and quality information on the web, there is every reason to believe that Wikipedia is a potential target. Among the billions and billions of harmless requests, there are without doubt some interesting ones, to filter out which is the NSA's specialty. Someone from the middle east is acquiring chemistry knowledge on Wikipedia that could be helpful in making bombs? A French author writes elaborate articles about military radio stations? The simple fact that most of what is accessed is harmless does not mean that everything is.

As a result, the privacy of our users is in jeopardy. Even if you don't agree with this, certainly the *belief in privacy* is in jeopardy. If users can't or won't trust us anymore to distribute uncensored information in a privacy-respecting manner, this is a huge loss. It is our responsibility to make sure that users can and will keep trusting and that their trust is well-founded by doing everything in our power to make sure our user's rights are respected. --Tobias talk · contrib 23:00, 16 June 2013 (UTC) Ps.: The big Internet companies are busy finding sneaky wordings that dodge the question of whether violated user privacy. With SOPA and PIPA there was a broad alliance. With PRISM, much more depends on our voice.

> Saying Wikimedia ought to take a stand whenever "the *belief in privacy* is in jeopardy" would seem to place an extraordinary burden on the foundation. One could point to a whole slew of legislation/government practices which potentially threaten the *belief in privacy*. Is Wikimedia's role that of some kind of privacy warrior akin the ACLU? NickCT (talk) 14:46, 17 June 2013 (UTC)
>
>> Sorry, I should have been more precise. I'm talking about privacy *when accessing Wikipedia*. Facebook and Google doesn't respect user privacy, that much is well known and it shouldn't be a great concern to Wikipedia/Wikimedia. Similarly, if the government decides to install more CCTVs, it doesn't impact Wikipedia directly. But with PRISM and other governmental spying activities, privacy not only of our users in general, but *while browsing Wikipedia* is at stake. --Tobias talk · contrib 18:48, 17 June 2013 (UTC)

## Snowden as Wikimanias keynote speaker [edit]

In August we will have Wikimania in Hong Kong and I would like to hear Snowden. (If it is secure for



Wikimania or Blue Lagoon?

him.) This would be also a good statement, beside joining stopwatchingus. So please invite him. --Kolossos (talk) 18:39, 17 June 2013 (UTC)

+1 --Kellerkind (talk) 19:00, 17 June 2013 (UTC)

+1 --Tobias talk · contrib 19:46, 17 June 2013 (UTC)

+1 --Manastirile (talk) 20:14, 17 June 2013 (UTC)

+1 -- TheOriginalSoni (talk) 04:20, 18 June 2013 (UTC)

+1 but not billed as a "keynote speaker". That's too big a statement, and I'd be very uncomfortable pinning our public face to this issue. While it's relevant, important, appropriate and will surely catch the media, our core Wikimedia priorities include our own affairs - Wikipedia Zero, global south, editor rates, Wikimedia community, Visual editor, and chapter and foundation highlights of the year. If we include a prominent but not keynote session with him, that doesn't dominate our core issues, that would come across better and more maturely - and not like bandwagon jumping. It won't go un-noticed for low-keying it. FT2 *(Talk | email)* 13:32, 18 June 2013 (UTC)

I don't imagine this will be possible. It seems as though Mr. Snowden is currently in hiding. I imagine by August he'll be in a U.S. prison or dead. --MZMcBride (talk) 16:50, 18 June 2013 (UTC)

...or in Iceland at the Blue Lagoon <:o) --Kellerkind (talk) 18:34, 18 June 2013 (UTC)

If it's unsafe for him to come personally, can he give a speech through Skype or something Ypnypn (talk) 22:26, 18 June 2013 (UTC)

+1, A dedicated speech will be more than enough. Chenxiaoqino (talk) 13:00, 19 June 2013 (UTC)

+1. I would suggest that he should be strongly encouraged to spend at least *some* time talking about how NSA surveillance affects Wikimedia projects in particular. In this way, such a talk can be viewed not solely as a political statement but as a technical consultation, and if an honorarium is required it would be more feasible to justify the spending on that basis. Wnt (talk) 21:23, 19 June 2013 (UTC)

- Though I should emphasize about the above that some good lawyers had better check over everything carefully - we would not want Wikimedia to end up with Assange-like charges of actually paying for/conspiring in *new* releases of classified information. Wnt (talk) 21:33, 19 June 2013 (UTC)

## Historical Background [edit]

See also w:Cabinet noir. One of the best things Wikipedians can do about this issue is to provide professional, serious, published knowledge about this issue in its articles. Teofilo (talk) 22:00, 17 June 2013 (UTC)

[edit]

## Call for input on WMF privacy policy

Not the same topic but related in many ways so I wanted to drop a note here pointing to the new Call for input on WMF privacy policy (also posted as a blog post) and it's associated discussion page. Jalexander (talk) 09:41, 19 June 2013 (UTC)

## Universal Declaration of Human Rights [edit]

> « *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* » (article 12).

Does anybody remember the Declaration of the Independence of Cyberspace? It was in 1996. Twenty years later, non-free software providers let governments to read everybody's emails, phone calls, web access… This is not only an attack against human rights, but also a threat to the knowledge society. Privacy is a pillar of liberty, a need on Internet. And without freedom, no free software. Mediawiki is free software, and our free encyclopedia is online.

We have to support our allies. (GENIUM ) 21:48, 20 June 2013 (UTC)

## and now? [edit]

A decision should be reached on the 21th June, now is the 25... Any news on the subject? --Isderion (talk) 01:38, 25 June 2013 (UTC)

Hello Isderion, we are reviewing the above comments, and we will share an update soon. Many thanks, Stephen LaPorte (WMF) (talk) 16:23, 25 June 2013 (UTC)

Soon? --Kellerkind (talk) 14:12, 2 July 2013 (UTC) P.S. If you don't like to do something, that's ok, but say something.

This is getting frustrating. You give the community one week to comment, the community participates to a small degree and then you need more than 2 weeks for reviewing the comments and reaching a decision. In the meantime you give no information to the community. This is not my understanding of a professional community liaison. --Isderion (talk) 23:14, 4 July 2013 (UTC)

Is there anything I can do to help here? I also haven't heard any update but, as I noted more generally here, I feel it is important to our community and to our long-term mission for us to take a stand beside like-minded organizations. I would like to help the WMF take a more public stance on the matter. –SJ talk 20:55, 7 July 2013 (UTC)

Thanks for the offer (and btw. congrats for the board seat), but the WMF posted an update 2 days ago, though it is a little bit hidden in the middle of the page (see Talk:PRISM#Update). It seems that this topic is rather low priority for the WMF, but I appreciate that they are going to focus on an international perspective, now that it becomes more and more clear that most governments spy on each others citizens and sometimes also their own. Maybe Noam Chomsky is right when he says that Governments will use whatever technology is available to combat their primary enemy – their own population :( --Isderion (talk) 22:21, 7 July 2013 (UTC)

## PRISM in not everthing [edit]

Now we have also a problem with British GCHQ so the problem comes to europe. And there are also articles about surveillance of public social media http://www.wired.co.uk/news/archive/2013-06/26/socmint and other stuff. So should we have different pages, should we have a more generally page or should we still concentrate on US-GOV and PRISM? --Kolossos (talk) 22:02, 26 June 2013 (UTC)

> Government surveillance? --Kellerkind (talk) 11:52, 27 June 2013 (UTC)

## Wikimedia may be lying [edit]

It is of knowledge of everyone that US authorities have, nowadays, power enough to make secret subpoenas, that means, request user's informations without user's knowledge, and without and order from a judge. The holder of the information may be arrested and suffer bitter consequences from revealing information about the subpoena to the targeted user. That said, subpoenas may have been sent to Wikimedia Foundation, and if it is forbidden to reveal any cooperation with US authorities, it's completely useless to simply state that it did NOT cooperate with them. Useless, and senseless, for the simple fact that it would be a crime to admit the oposite. That said, it is clear for me that it is **NOT** safe to trust in ANY organization, foundation or enterprise located in the US, or owned by any US organization, foundation or enterprise. US has become a state of exception, and the most realistically measure to be taken would be moving not only servers, but also capital, staff and headquarters to places where freedom of expression still has some meanning.

- AFAIK with open source software it's harder to hide secret measures to record information than with closed source software. The Wikimedia software on this site is open source. It's why hackers didn't trust Michael Domscheit-Berg when he refused to release the source code for his "en:OpenLeaks" website. WhisperToMe (talk) 15:02, 6 July 2013 (UTC)
    - It is possible for certain requests (*national security letters*, which are different than a subpoena) to include a demand that you not tell anyone you have received one. However it does not compel you to lie; you can simply say you "cannot answer" when asked whether you have received one. In contrast, until an organization has received such a request, it can say clearly that it **has not** received such a request. Wikimedia's head counsel stated clearly on the blog, "*We have not received any National Security Letters*." (Caveat: as a Board member, I would not be notified if such an NSL had been received by the Foundation, so I have no direct knowledge.) –SJ talk 20:55, 7 July 2013 (UTC)

*The above discussion is preserved as an archive. **Please do not modify it.** Subsequent comments should be made in a new section.*

## Further feedback and suggestions [edit]

## Copied from above [edit]

Hello all, thank you to everyone who shared their feedback above. Based on this consultation, there is limited support for advocacy about government surveillance, such as PRISM. We are currently evaluating possible advocacy options that are consistent with this feedback. Particularly, we are looking for options that are focused on government surveillance from an international perspective. You are welcome to continue to leave feedback and suggestions, and I will keep you updated. Thanks again, Stephen LaPorte (WMF) (talk) 18:52, 5 July 2013 (UTC)

15 threads, 10 support, 1 comment, 4 oppose (66.7%, 6.7%, 26.7%) - Amgine/meta wikt wnews blog wmf-blog goog news 17:28, 8 July 2013 (UTC)

But also a fair amount of negative feedback in other parts of the discussion (e.g., "US Issue" below, some of the blog comments), so my sense is that a pure count of the (very small) numbers does not mean much. Honestly open to persuasion/discussion on that point, though. LVilla (WMF) (talk) 17:39, 8 July 2013 (UTC)

Actually, I took the liberty of examining the remainder of this page. Not one thread did I find which stated opposition to action on this topic. There were questions about whether this is a a solely US topic (which, in a manner of speaking, it is, as it's the US NSA whose actions are being discussed.) There were discussions which suggested this is diversionary. But none opposed acting on it. Perhaps you're referring to discussions elsewhere and ascribing them locally as none expressed opposition to acting on this topic as far as I could discern. - Amgine/meta wikt wnews blog wmf-blog goog news 07:03, 9 July 2013 (UTC)

As one of the first commenters on this page, I said:

> "This certainly seems like a fad issue. [...] I think working on documents such as User:Sue Gardner/Wikimedia Foundation Guiding Principles is a much better use of time and other resources. This allows us to define what we stand for and what we believe, rather than simply denouncing whatever the latest government abuse (or potential future abuse) happens to be in the news at the moment (SOPA, PRISM, etc.)."

If this isn't explicit enough to rise to the level of stated opposition to action on this topic, let me know and I can rephrase.
Another comment copied over to this page reads:

> "Should Wikimedia join in decrying PRISM? No."

Given comments like these, I'm not sure what opposition to action would look like to you.
It would be helpful if you could describe specifically what actions you feel the Wikimedia Foundation should take and how you feel those actions would further the Wikimedia Foundation's mission. I think most Wikimedians strongly disagree with secret government surveillance programs such as PRISM. But what of it? Wikimedia is in the business of providing free educational content to the world, not acting as a freedom fighter or political advocate. --MZMcBride (talk) 19:43, 10 July 2013 (UTC)

If we feel that "stopwatching.us" is too US-centric, I think it would be appropriate for us to post a similar statement of our own, framed more globally.

- Indicating that we will support regional or national efforts to keep this aspect of the web open, because of its impact on the free exchange of knowledge.
- Listing the national/regional initiatives we are aware of, which we may or may not have expressly signed on to.
- Listing and amplifying the participation of Chapters and other regional Wikimedia groups who have supported those regional initiatives.
- Encouraging the global Wikimedia community to help keep the Web open in this fashion.

–SJ talk 18:34, 8 July 2013 (UTC)

> I think making a public statement that is less US-centric is fine as well and more in line with our global mission. --Tobias talk · contrib 11:31, 13 July 2013 (UTC)

### Followup blog post [edit]

FYI, the Foundation/LCA wrote and posted a followup post on this topic on July 18.

## We should sign the global Principles on Surveillance guidelines [edit]

A coalition of global groups, called "Necessary and Proportionate", formulated a beautiful and non-nation-specific set of guidelines for how to apply human rights principles to surveillance.

It is called the "**International Principles on the Application of Human Rights to Communications Surveillance**", and has been signed by hundreds of organizations, including human rights, internet, legal, policy, and knowledge organizations. This would be an excellent and appropriate statement for us to sign.

We would be the largest website to sign on to date; but dozens of major global organizations and foundations that we rely on and work with have already done so. –SJ talk 00:56, 7 November 2013 (UTC)

> I am very supportive of this suggestion. How can we learn what is the status of the Foundation's decision-making on this suggestion? - Amgine/meta wikt wnews blog wmf-blog goog news 04:57, 6 December 2013 (UTC)

## Meu temor(como brasileiro): [edit | Add topic]

- Eu acho que o governo americano podem invadir conta de administradores da wiki e destruir este projeto. Por isso defendo que sites como o nosso tenham o sistema de segurança EV-SSL. João bonomo (talk) 17:13, 19 July 2013 (UTC)
- I think the U.S. government can invade the wiki administrators account and destroy this project. therefore argue that sites like ours have the security system EV-SSL. João bonomo (talk) 17:13, 19 July 2013 (UTC)

This page was last edited on 6 December 2013, at 04:57.

Use for details.

Privacy policy About Meta Disclaimers Developers Cookie statement Mobile view