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

Plaintiff’s Exhibit 9

Talk:Access to nonpublic information policy/Archives/2013

< Talk:Access to nonpublic information policy

***Please do not post any new comments on this page.** This is a discussion archive first created on December 9th 2013, although the comments contained were likely posted before and after this date. See current discussion or the archives index.*

Internal policy on ID collection

This was posted by Geoff on the Privacy Policy talk page but I think would be interesting to those here as well.

> **Wikimedia Foundation - Internal Policy**
>
> **Purpose**
>
> The Wikimedia Foundation ("WMF") may sometimes need to collect copies of identification documents ("IDs") from community members pursuant to established policies of WMF or the community. Examples where community members may need to identify themselves include the following:

Contents

- Candidates (http://meta.wikimedia.org/wiki/Board_elections/2011/en#Prerequisites_to_candidacy) for the WMF Board of Trustees
- Candidates (http://meta.wikimedia.org/wiki/Funds_Dissemination_Committee/Framework_for_the_Creation_and_Initial_Operation_of_the_FDC#Membership) for the Funds Dissemination Committee
- Recipients of WMF grants
- Representatives and agents of user groups and thematic organizations
- Community members (http://wikimediafoundation.org/wiki/Access_to_nonpublic_data_policy) with access to nonpublic user data information [GRB Note: we are currently not keeping such IDs on file.]

This internal policy summarizes the approach to be taken by WMF employees and contractors when handling and storing such community member IDs. The required ID depends on the criteria of the particular policy or practice, but may include copies of passports, driver's licenses, and other government-issued documents showing real name and age.

Collection, Storage, and Access

Copies of IDs provided to WMF by community members will be kept confidential, consistent with any applicable requirements of the WMF privacy policy (http://wikimediafoundation.org/wiki/Privacy_policy). Physical copies of IDs will be kept in locked cabinets designated for this purpose. Electronic copies of IDs will be protected by passwords or other electronic protections in files designated for this purpose.

Access to IDs will be limited to a "need to know" protocol determined by the program administrator. Usually that means only the principal administrators of a program will have access to those IDs. WMF will not share the IDs with outside third parties, unless required by law, covered by a non-disclosure agreement approved by Legal, or necessary to protect the rights, property, or safety of WMF and its employees and contractors.

Destruction

IDs will be kept as long as necessary to satisfy the need of the applicable policy and practice requiring the IDs. Such IDs will be destroyed as soon as the need for the ID has expired. Depending on the program, some IDs may need to be retained for a period of time for legal and financial purposes beyond the immediate purpose of the policy and practice. For example, IDs may need to be retained after the life of a grant to prove expenditure responsibility to government officials in the case of an audit. Check with Legal and Finance for any legal or finance record retention requirements.

V.1.1 (2013-03-14)

Illustrations

The following discussion is closed.

There are obviously a lot of things to talk about and if you aren't interested in this piece of it please feel free to start a new section with your discussion point/question/concern/etc. As you can probably see both here and on some of the other policies and draft pages we rolled out we're trying the idea of having illustrations and light humor in the text. These are not in anyway 'set' and may not appear in the final version if they're not appreciated. Legal documents tend to be lengthy, weighty and difficult to read (and rarely read at that) especially when you consider how many sites the average user visits. We want to make these documents as accessible as possible to as many people as possible. We hope to keep everyone's attention with the illustrations and a bit of levity. This is especially the case in the privacy policy but we've seeded them in a couple other locations as well. Do you like them? Hate them? Any specific ones work well or not work well? Should we think about another scene for a specific area? Jalexander (talk) 23:07, 3 September 2013 (UTC)

> I think the icons in the Privacy Policy are fantastic. Clear, and highly useful for navigating sections. The illustrations in both are fun, and I generally like them, but they're less useful for communicating the subject of the section. The top of the document says Rory is there to help explain the policy, but it doesn't feel like he's a narrator, more like an adornment. I think he should either be more tightly-integrated (perhaps with full SVG and color) or done away with in the name of simplicity. Steven Walling (WMF) • talk 05:18, 4 September 2013 (UTC)
>
>> I know color etc is an option for the final, it was just sketches now as the intro. Are you thinking more 'narration' ? Jalexander (talk) 05:20, 4 September 2013 (UTC)
>>
>>> Yeah I think if there's going to be a character, narration is probably more useful. Having to describe each section by putting it in a caption for the character to say is probably a good exercise in distilling the policies. Steven Walling (WMF) • talk 05:31, 4 September 2013 (UTC)
>>
>> The sketches of Rory are actually also meant to be up for community feedback -- the sketches are meant to be a start (that's actually why he is not in color and is unfinished). Final drafts of Rory will only be completed once community input has been obtained. We'd love to hear how he could be better utilized. Do you (the community at large) like the proposed sketches? Do you have ideas as to what else he should be doing to illustrate the concepts in the policy? What kind of narrative can we give him to bring the policy to life? How he could be better integrated? Privacy policies are notorious for being unreadable and hard to relate to. We hope that, with the community's assistance, Rory will be able to help with that. Mpaulson (WMF) (talk) 07:07, 4 September 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:44, 3 December 2013 (UTC)

Who's we?

The following discussion is closed.

"We will be accepting community comment until 15 January 2014. We look forward to comments on any aspect of the draft." ← Who's we? --MZMcBride (talk) 04:56, 4 September 2013 (UTC)

> Hi MZMcBride! "We" refers to the Wikimedia Foundation. This draft was the result of a collaborative effort between different departments, and coordinated by LCA. But the draft is not and cannot be complete without community input. We hope to hear from you during the community consultation period between now until 15 January 2014. During and following the community consultation period, we will be editing the draft presented today to reflect community suggestions and concerns, as appropriate, and then present the final draft to the Board for discussion and approval. Mpaulson (WMF) (talk) 05:15, 4 September 2013 (UTC)

A general aside: thank you so much for organizing these thorough public discussions and taking all of the feedback into consideration. I am learning a lot from this; and other community processes could as well. Including most of our global RfCs. –SJ talk 21:55, 24 October 2013 (UTC)

> Thanks Sj! The documents we introduce to the community are only a starting point. We learn so much from the community's participation and feedback during this process, and any resulting policies are better for it. =) Mpaulson (WMF) (talk) 22:15, 24 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:45, 3 December 2013 (UTC)

Wikipedia Day 2014

The following discussion is closed.

"We will be accepting community comment until 15 January 2014." ← What happens after January 15? Is there a public timeline anywhere? I assume at some point the Board has to approve the policy. --MZMcBride (talk) 04:57, 4 September 2013 (UTC)

> Hi MZMcBride! This draft is just that, a draft. We are working towards completing a final draft that has gone through vigorous interdepartmental and community feedback and will present that eventual draft to the Board for their review and discussion. The draft presented today will be reviewed and revised throughout the community consultation period in light of community feedback. After 15 January 2014, the draft will undergo any final revisions based on community feedback that

are still needed and then will be presented to the Board for discussion and potential adoption. Hope that helps! Mpaulson (WMF) (talk) 05:31, 4 September 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:45, 3 December 2013 (UTC)

Protect your access

The following discussion is closed.

Should contain something alla: 'users with these responsibilities will do the utmost to protect their accounts against unauthorized access, report immediately when they are aware such access has been compromised and follow the current agreed upon standards of usage of the account', the latter indicating that a user should use https if so defined in the current rules for checkuser access for instance. So i want to express that users can be assured that these people have a certain set of rules that they need to follow in order to be checkuser for instance, other than the 3 requirements of 18, ID'ed and pledged to confidentiality. TheDJ (talk) 07:01, 4 September 2013 (UTC)

Hi TheDJ! Thank you for your suggestion. Some of your concerns are actually addressed in the Confidentiality agreement for nonpublic information already.

As to your first suggestion, users with these responsibilities must "Comply with the Privacy Policy; the Access to Nonpublic Information Policy; and any other applicable and nonconflicting community policy relating to nonpublic information" and "Refrain from disclosing nonpublic information to anybody, except as permitted under those policies". Do you think adding another requirement that they must generally strive to protect their accounts against unauthorized access in addition to the requirements I mentioned above would be beneficial?

As to your second suggestion, they also have the duty to report disclosures under the terms of the confidentiality agreement -- they must "Notify check-disclosure at wikimedia.org and provide an explanation within 10 days if [they] disclose nonpublic information to outside parties, such as law enforcement" and "in case of a violation of this agreement, including improper access, use, or disclosure of nonpublic information...[they] will notify the Wikimedia Foundation about the violation immediately".

And finally, regarding your third suggestion, there are currently discussions within the Foundation as to how we can provide more secure connections to users with access to nonpublic information, but a perfect solution has not yet been found. https is certainly an option, but not one that we can apply everywhere. For example, https can actually hinder a user's ability to access in certain countries, like China. Your suggestion is a good one and one that we would like to implement in the future once we have methods of providing more secure access to users with these responsibilities (and hopefully all users eventually). Mpaulson (WMF) (talk) 18:13, 11 September 2013 (UTC)

In hindsight, I don't care as much about those 3 specific things, they could be internally documented. I want to make it clear to readers that the people who have this access to private material are required to act following the operational guidelines that are set for their specific 'position'. If you have "Minimum requirements for community members applying for access to nonpublic information rights", then (a) is a eligibility requirement for the functionary, (b) is an identification requirement on the functionary, (c) is an ethical agreement that the functionary signs with the foundation (which represents the community), (d) is a requirement onto the foundation about the proof talked about in a, b and c. My statement would have to express the 'burden' that is placed onto the functionary when he operates in his function to operate with the methodology that is expected of the function/office. (this could then include requirements on using https all the time for instance, protecting your password in general etc, but also for instance keeping non-public logs of actions for instance). We have trusted these users with some access and we require them to be careful with that access. When the library lends you a book, you don't bring it back all torn up. I don't know, it's complicated :D TheDJ (talk) 13:19, 23 September 2013 (UTC)

That's a fair point. What about if we change the last bullet point under (c) to "when and to whom they may disclose the nonpublic information and how they must otherwise refrain from disclosing nonpublic information to anybody, except as permitted under applicable policies" and add an additional bullets point saying "how they must safeguard their accounts from unauthorized access" and "when they must report disclosure of nonpublic information to third parties or improper access, use, or disclosure of nonpublic information"? We could would also add an additional bullet point in the confidentiality agreement under the "Protection of nonpublic information" section stating "Reasonably safeguard your account from unauthorized use." Let me know what you think of the additional language. Mpaulson (WMF) (talk) 23:47, 15 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:51, 3 December 2013 (UTC)

Why should copies of the photos ID be retained ?

The following discussion is closed.

While I can understand that the WMF would in some cases need to have confirmation of the identify of a volunteer, it is not clear to me why it should keep a copy of the actual photo ID. Whenever I need to be authenticated, I show my ID, someone checks that the information they have recorded is correct, then ticks a box on a paper form saying "ID checked" and confirms by signing it -- without keeping a copy of the ID. Usually, only banks require an actual copy of the ID. Why wouldn't it work ? In Switzerland, sending a copy of a photo ID is enough to authentify oneself in order to get access to most documents (medical record, bank accounts, criminal record). However, simply knowing the information printed on the ID does not open any such door. Could we setup the system in this way ? I know that the probability of someone misusing the data stored at WMF is small, but the potential consequences in case of problems are **huge**.

Another scheme that was suggested a while ago is that chapters (in countries where they exist), or a lawyer mandated by the chapters, should/could be used as a trusted 3rd party that would authentify such photo ID and send the relevant information to the WMF. This would have the added advantage that, for quite a few volunteers, they would not have to send any document to a foreign country (they may not even have to make a copy of the photo ID). Additionally, local people know what official photo IDs look like, and they could see the original document, reducing drastically any possibility of fraud. To me, this sounds like an appealing scheme, no ?

Finally, I am wondering about the following sentence:

> *The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department*

I read that as "the WMF will not share submitted materials with third parties, except when it has itself approved to do so". That seems like a very weak protection. Shouldn't there be a explicit limitations of the cases in which such a transfer of material can happen ?

Thanks in advance ! Schutz (talk) 09:24, 4 September 2013 (UTC)

FWIW, that's *not* an appealing scheme to WMIT, as clearly stated by our president and board. Of course if the WMF hired EU firms to handle such stuff many would be happier. --Nemo 21:04, 4 September 2013 (UTC)

Which problems do you see with this scheme ? Legal, practical, others ? Schutz (talk) 09:14, 5 September 2013 (UTC)

WMIT doesn't want and can't be an *agent* of WMF for anything. --Nemo 12:30, 5 September 2013 (UTC)

Hi Schutz! One of the main reasons we are requiring identification from community members with this level of access is accountability. The information that is entrusted to these community members is very sensitive and knowing who has access to that information is a big part of working towards accountability. In the examples you stated where identification is required to get access to other information, you presumably get checked every time you try to access that secured information. Here, in situations covered by this policy draft, where the access is continuous, retaining a copy of the id submitted seems more logical that attempting to check someone's id every time they attempt to exercise their access rights.

As to your second comment about whether it should be WMF that holds the ID, Nemo is correct in that chapters should not be seen as agents of WMF. That also doesn't help the community members who do not have chapters in their countries (or if in their countries of residence, chapters that are geographically close to where they reside). Appointing third-party attorneys or bodies to collect and hold the ids locally is administratively and legally challenging as well. Do we appoint an attorney in every location where there is a community member who submits an id? If the attorney is appointed, who is the attorney's client -- the community member or WMF? How would be ensure that all of these attorneys retain a copy of the ID properly (both in length of time and with proper security measures in place)? What happens if an attorney leaves practice and doesn't tell us or the community member? We believe that whatever risk associated with WMF's storage of the ids is considerable less than if the ids were stored by third parties.

And finally, as to your third comment, I think some clarification about what kind of situations the sharing of these materials section is meant to cover will help guide this discussion. First, though, I'd like to note that there are limitations on when we can share the materials with third parties, specifically: "(B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." Do you believe these situations are reasonable?

I do understand your concern with regard to "(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department" though. The reason why we included this was to address situations where a person helping with security of the materials is a contract employee who has signed a non-disclosure agreement with the Foundation or if we hire a company (who has signed a non-disclosure agreement) to help secure materials submitted electronically and they have to handle the materials in the course of helping us. The point of the Foundation's non-disclosure agreements with these sorts of parties would be to secure similar or greater protections than those promised in this policy. Does that make sense? If so, do you think the language of (A) could be changed to make this clearer?

Hope this helps and look forward to hearing more of your thoughts on these topics. Mpaulson (WMF) (talk) 20:13, 11 September 2013 (UTC)

Sections (A) and (D) jumped out at me as well. They both appear to offer quite fragile protection for those submitting "non-public information" to the WMF - which is, you might agree, ironic. I think A should be tightened up to narrow the circumstances in which information is shared (such as including provisos that it will not be for commercial use, and that no outside entities will retain a permanent copy of any personally identifying information). I think D also has holes big enough to drive a truck through, because "rights and property" of the WMF, its employees and contractors is a pretty broad category. Does that mean if permanently deleting the data from the hard drive of a contractor might damage that contractors property, the policy allows them to retain the information? I understand that the natural inclination of attorneys representing a client is to draft as broadly as possible in favor of the client, but that is the wrong impulse when considering the responsibility of the WMF to protect the identifying information of both readers *and* volunteers. Since the volunteers are potentially sharing much more sensitive information, a little more weight on protecting them needs to be added to this policy. **Nathan** T 19:25, 14 October 2013 (UTC)

Hi Nathan! Thank you for sharing your thoughts. As to (A), what do you think about tightening the language to something like this: (A) permitted by a non-disclosure agreement that (1) has been approved by the Wikimedia Foundation's legal department; (2) allows for only non-commercial use of the submitted materials; (3) allows for use by the recipient of the submitted materials in accordance with the Wikimedia Foundation's instructions; and (4) obligates the recipient of the submitted materials to return or destroy all copies of the submitted materials in its possession within a reasonable time following the recipient's need for the information.

And as to (D), I understand why you think the provision is broad. It is meant to be, but not because we are trying to draft broadly in favor of WMF as our client. We wrote it broadly because it was meant to cover unlikely and, to a certain extent, impossible-to-predict scenarios that can be hard to enumerate. I admit, I'm a little confused by your example of how this provision could be used. If permanently deleting the data from the hard drive of a contractor would damage that contractor's property, that doesn't mean that the policy allows them to retain the information. Clause (A) would cover how we were permitted to give access to the information to the contractor, but not how long they could retain the information. Clause (D) covers completely different scenarios where we would be permitted to share information. For example, in the unlikely scenario where our building was broken into and our equipment was stolen or where our computer systems had been compromised and we had a good reason to believe that it was someone whose personal information we had, we would be permitted under this clause to report that person to the appropriate authorities. Again, it's hard to imagine every possible scenario where this clause may be helpful. I frankly hope we never, ever have to use the clause. We do not take the disclosure of personal information lightly. In fact, we are loathed to disclose information short of being legally compelled to do so or for safety reasons. That said, we're very much open to editing (D) in a way that would better illustrate what that clause is trying to cover and I'd love to hear any suggestions you may have. What about something like this: (D) needed to protect the safety of others or WMF staff, contractors, systems or property?

I look forward to hearing your thoughts on my suggested revisions as well as any suggested revisions you may have. Mpaulson (WMF) (talk) 19:54, 16 October 2013 (UTC)

You still have not answered the question of why the ID has to be retained over retaining the Data in it. And I for one will never, ever accept the property clause of this proposal. That is simply unacceptable. ***Snowolf*** How can I help? 20:07, 17 October 2013 (UTC)

I second Snowolf's sentiment; I don't think our data should be used for non-commercial purposes, either. I also suggest to obligate any recipient of our sensitive personal information to return or destroy all copies *immediately* following their need for it. On a related note, why would you share this sort of personal information with anyone at all? I don't really see any need for any contractor or WMF staff member except perhaps two or three people (take Philippe and Geoff from Snowolf's example above) to have access to it. odder (talk) 21:08, 17 October 2013 (UTC)

Outside counsel is the only thing I can think of. ***Snowolf*** How can I help? 21:28, 17 October 2013 (UTC)

"You still have not answered the question of why the ID has to be retained over retaining the Data in it." I think we'd probably be OK with simply retaining the data. We'll have to think about it some more, but the ID portion of the proposal was mostly based on past practice. Would keeping data, rather than the ID, resolve your other concerns about us collecting this data? -LVilla (WMF) (talk) 22:43, 25 October 2013 (UTC)

On the question of "property" as a "loophole": the idea here is really primarily about our technical infrastructure; e.g., if a volunteer developer who we have ID'd starts attacking the site, we'd like to be able to use this information to help identify them and protect the site. So does it feel more narrowly tailored if we replace "property" with "infrastructure"? -LVilla (WMF) (talk) 19:57, 1 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:51, 3 December 2013 (UTC)

CheckUser policy

The following discussion is closed.

As already addressed here, let me reiterate my remark (that still remains) about the revelation of **the link** between an IP and an account, as it is a compound of private and public data.

Aside from this point, I am happy with the changes and the new layout of the page. Elfix 08:00, 5 September 2013 (UTC)

Hi Elfix! Just to be clear, are you referring to the the link between logged-in accounts and anonymous accounts in situations like sock-puppet investigations? If so, I think the Privacy Policy draft most directly addresses this situation in the To Protect You, Ourselves, and Others section...specifically: "We may need to share your personal information if we reasonably believe it is necessary to enforce or investigate potential violations of our Terms of Use, this Privacy Policy, or any Foundation or user community-based policies." To a certain extent, public inference of the links between particular IPs and accounts are unavoidable in sock-puppet investigations and are permissible due to the sentence above. I do understand your concern that it is not as clearly stated with in the Access to nonpublic information policy draft or the Confidentiality agreement for nonpublic information as to whether the community members handling these investigations are permitted to disclose this information in the course of their investigation. I'd love to have this stated more clearly. Do you have any suggestions as to how we could make it clearer in either the Access to Nonpublic Information Policy draft or the Confidentiality Agreement draft? Mpaulson (WMF) (talk) 19:28, 11 September 2013 (UTC)

Thank you for your response. I didn't pay enough attention to the bit you are quoting, and it is, I think, clear enough. Thanks! Elfix 21:33, 12 September 2013 (UTC) However, in "We may need to share your personal information", the use of the "share" verb may not be clear here (share with whom?). Elfix 18:50, 13 September 2013 (UTC)

Yes, the language in the Privacy Policy draft is relatively broad because it's trying to cover any possible person/entity that may have to be alerted depending on the type and severity of the alleged violation committed by literally anyone who can access the Wikimedia Sites. I'm not sure if there's a way for us to do an exhaustive list to cover every possible scenario. We do try to be more specific in the Access policy draft about to whom and under what situations community members with access rights may disclose information to though. Mpaulson (WMF) (talk) 00:36, 16 October 2013 (UTC)

I have a follow-up hypothetical question for you. The case of the UK where random IPs in dynamic ranges typically don't do anything other than reveal you're in the UK is quite clear cut. However, let's say that a person's IP reveals private information about them (e.g. they're on 130.88.0.0/16, a range owned by the University of Manchester). In terms of the policy, does this change the above advice that it's permitted to disclose that IP to someone in the case that they, say, want to write an abuse complaint to the University of Manchester? --Deskana (talk) 09:25, 15 October 2013 (UTC)

Hi Deskana! Thank you for your question. Do you mean whether it would be ok for a community member with access rights to disclose a nonpublic IP that is specific enough to identify that the IP falls within a range owned by the University of Manchester and is associated with a user account? It would be ok if the disclosure was made as part of an investigation of potential violations of a policy and the IP was disclosed in the an abuse complaint "to assist in the targeting of IP blocks or the formulation of a complaint to relevant Internet Service Providers" (that latter if UM was also the ISP). Otherwise, no, they should not disclose the IP. Did I understand your hypo correctly? Mpaulson (WMF) (talk) 00:36, 16 October 2013 (UTC)

Perhaps a more specific and common situation: IP address provides some sort of information about the user (e.g., it's a business IP, and researching it through WHOIS will identify the business). There are a pile of socks, and there are no good users on the IP. Standard practice is to at least softblock the IP while also blocking the socks. However, it takes no imagination at all to make the association with the IP address and the socks just by looking at the CU's block log. So....is the CU violating policy by blocking both the socks and the IP? Risker (talk) 02:27, 16 October 2013 (UTC)

Hello @Risker:, this is a tough situation. For the same reason that Michelle explained above, it's allowed under the current version of the policy. However, upon a closer reading of the new draft privacy policy and access to nonpublic information policy, this is not addressed directly. To make it clearer, we could add to "Use and disclosure of nonpublic information", section (b):

> *Disclosures of nonpublic information may be made to: ... the public, when it is a necessary and incidental consequence of blocking a sockpuppet or other abusive account; ...*

This would make it acceptable under the privacy policy/access policy for CheckUsers to conduct the type of blocks that you suggest. Of course, projects could also set a higher bar in their local CheckUser Policy, if they don't think this is appropriate. This is a tough question, but the policy can be accommodating if its necessary for CheckUsers to do their job. Thanks, Stephen LaPorte (WMF) (talk) 21:13, 1 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the fact that it appears to be resolved I'm going to archive this in a couple days unless reopened. Jalexander--WMF 20:54, 3 December 2013 (UTC)

Data retention forced by what law?

The following discussion is closed.

Current draft says the collected ID will be retained for 3 years. I'd like to ask this measurement is forced by what law. In my country the data retention criteria are fixed in written law, and unless the data retention is required by law the data must be destroyed immediately the purpose of data collection is satisfied. Data retention without legal basis will be only the risk that the data would be compromised. There are several accidents that personal information of 35+ millions of people are leaked. If the data retention is based on US law, please let us know where the legal basis is, and if not, please don't retain the data. Best regards. – Kwj2772 (msg) 14:34, 25 September 2013 (UTC)

The same here in Italy, data must be destroyed *as soon as possible* on request. --Vituzzu (talk) 18:30, 14 October 2013 (UTC)

I doubt the specific time period is mandated by law, although there are various statutes of limitation - many of which in California are three years or less. I'm just speculating, but other circumstances that might dictate data retention times are contracts, grant terms, government funding, participation in certain state or federal programs, etc. Unlike European and other jurisdictions, the U.S. does not have a general limit or prohibition on retaining private data. And while many users live in jurisdictions where those rules apply, they do not govern the behavior of the WMF. **Nathan** T 19:37, 14 October 2013 (UTC)

But still I'm subjected to EU law. --Vituzzu (talk) 10:46, 15 October 2013 (UTC)

Hi Kwj2772, Vituzzu, and Nathan. Thank you for your questions. While there are data retention periods that are mandated under US law for specific situations (such as tax purposes, retention of client files, etc.), Nathan is correct in that there is no general law in the US that governs data retention periods and WMF is not subject to EU retention laws. Organizations are free (absent specific situations where particular laws apply) to set their own data retention periods for different types of data. Mpaulson (WMF) (talk) 17:49, 18 October 2013 (UTC)

Even if you're not subject to EU laws on data retention, it might be well worth looking into them and perhaps adopting some of the regulations; there are many stewards, checkusers, oversighters and OTRS members who are EU citizens, and I'm sure some of them would like you to adopt these higher standards even if you're not obliged to do so by U.S. law. odder (talk) 17:59, 18 October 2013 (UTC)

I would be interested in hearing from you guys about what you think would be an appropriate retention period? If you have thoughts on this issue, please leave them in the retention thread. (I'm trying to keep the responses on that topic in one place so they are easier to track.) Thanks! Mpaulson (WMF) (talk) 22:56, 25 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:02, 3 December 2013 (UTC)

Re-identification and retention of data vs. the NSA

The following discussion is closed.

I have identified to the Foundation a couple of years ago upon receiving access to OTRS, and my identification has been confirmed by a WMF staff member. Therefore, I cannot see anything that changed in those past few years that would require me to re-identify with the WMF, and send them a scan of my ID again.

I am also very concerned and feel deeply uneasy about (re-)sending a copy of my ID--which is probably one of the most delicate information the WMF can hold--to an organisation in a country where countless government agencies can force them to reveal any and all information they want, or even get the information without a court's approval or the subject's awareness. (Yes, I'm looking at the U.S., the recent scandals around the NSA, and the worryingly broad scope of the CIA and other intelligence-gathering organisations.)

If a re-identification or change of the current policy is required, I would prefer to be able to identify to an organisation, group or an individual acting in professional capacity in a jurisdiction which guarantees the best possible protection of my personal information (see data retention policy issue brought above by Kwj2772), and where I will have the ability to protect my personal liberty in the most effective way possible, without having to spend tens of thousands of dollars and fight against the ever-expanding appetite of government intelligence agencies. odder (talk) 16:12, 14 October 2013 (UTC)

This policy will make most of most active users leave the Project, I wonder who will eventually checkuser, oversight, etc upon these basis.

- These changes are made by a completely USA-centric perspective, without any care for other Countries' jurisdictions (for instance the three-years terms violates Italian law) but also different cultures (for instance in European countries law tends to avoid lawsuits and *subpoena is completely insane by our perspective*). You shouldn't forget users living outside USA are subjected to their respective countries' laws.
- These changes make the policy even more blurry, on a theoretically basis everything can be meant to *prevent damages to WMF's properties*.
- Also, a confidentiality pledge is not bad but still it doesn't take into any consideration the whole World outside USA, both the agreement and the way to sign it might have no value at all for people living outside USA.
- This new version gives legal value to "normal" emails, I don't know if this might have any value in USA, but this is utterly ridiculous here in EU.

Finally I have a simple question: each change is supposed to fix some practical problem, so, **which problems are supposed to be fixed by these changes?**
--Vituzzu (talk) 17:35, 14 October 2013 (UTC)

Hello @Vituzzu: Michelle has provided more detail on why these changes are being considered below, at Rethinking the access policy: Response to recent feedback. Does this answer your question? Stephen LaPorte (WMF) (talk) 21:39, 1 November 2013 (UTC)

- Anything could be argued to be a damage to WMF's properties. If I go out and criticize the WMF, I am damaging its properties in a way. I do not think that I would be able to continue serving in my capacities should such a flimsy policy be implemented. I was already uneasy about submitting identification when I did so some years back, and that was with the assurance that it would be destroyed after my identity was confirmed. My concerns are magnified by the idea of the documents being retained. I recall a lengthy thread on some OTRS mailing list in 2008 or 2009 about the processing of identification informations, where several volunteers were raising questions about the then current practices. Some of the points made then should be taken into account now, if the WMF wishes to go ahead with this. ***Snowolf*** How can I help? 18:08, 14 October 2013 (UTC)

It's also funny to read *WMF employees and contractors...hey I'm a contractor making a research about the way different countries print IDs!* Seriously, nobody knows how the fuck is hard to sue one of these unfaithful contractors from the other side of Atlantic or Pacific Oceans?
Also, though my main question still is "why is this change needed?" I have also another question: "why so few announcements have been made in comparison with the asphyxiating spam we are used to receive for every futile change in some useless MW's functionality?".
--Vituzzu (talk) 18:28, 14 October 2013 (UTC)

I'm more concerned about id theft and data leak than anything else. I don't like the idea of somebody storing a scan of my driver's license, which could easily be used for nefarious purposes by malicious individuals, on a networked server. Would the data be taken from the "secured" inbox, encrypted, and then placed into an air-gapped server? Reaper Eternal (talk) 18:40, 14 October 2013 (UTC)

That is my worry too. I also don't want the printed stuff to be in a some office locker. It should be in a serious safe. We should have a list of those with access, etc.. The issue of the air-gapped server was discussed at length in the otrs mailing list in a thread from I belive 2008 or 2009. I wish I could find it as the point made there are just as relevant now. ***Snowolf*** How can I help? 19:31, 14 October 2013 (UTC)

The discussion you seem to have in mind took place in February 2011. You can see the relevant thread on Wikimedia-l (then Foundation-l) here (http://lists.wikimedia.org/pipermail/wikimedia-l/2011-February/110390.html); there was also a discussion on the OTRS wiki cafe (https://otrs-wiki.wikimedia.org/wiki/Caf%C3%A9/Archive_6#Identification_of_OTRS_agents). This post on Foundation-l (http://lists.wikimedia.org/pipermail/wikimedia-l/2011-February/110392.html) mentions threads on the private otrs-en-l and otrs-permissions-l mailing lists, but I am no longer subscribed to any of them, so I can't check the archives. I hope this will help with your search. odder (talk) 20:19, 14 October 2013 (UTC)

I can only agree with odder, Vituzzu, Snowolf and Reaper Eternal. This proposal is highly outrageous. Like Vito I can't see any problem which would be fixed by this. I plan to resign as a steward if it passes. Some complaints, in addition to those already mentioned above:

- At first it is stated (in "(d)(i)") that the data will not be shared by the WMF etc. bla bla except if *(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors*. As wide-ranging as that is formulated, it st)ll gives some "severe" criteria. Then in the next section ("(ii)") however we read *"the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member."*
  - That the Foundation may need to contact a user about how/why he used CU in a certain way or so certainly does not always mean that they may need to do it to protect the Foundation's glorious property. Nevertheless just before such a requirement was established. So why is such a fishy reason used for justifying keeping the data? Even more dubios the next reason:
  - What the heck is a "user community committee"? The next sentence of course suggests it is "the Arbitration Committee". What the heck is "the Arbitration Committee"? There is no global arbcom or anything. Just some projects happen to have one. This proposal was clearly written by someone focussed on enwiki.... but apart from that, it sounds like any community may just establish a committee that then uuuurgently has to ask some questions. How nonsensical. If at all, there need to be clear criteria for such an (arb?)com - which criteria it must fulfill (e.g. selection method, identification of members themselves?) in order to be considered to be allowed access to such data.
  - Additionally, how would such a "the Arbitration Committee" contact the user? (It also of course seems like we must assume someone who is not active anymore, as otherwise he could simply be asked on his talk page or by mail. Right to vanish?). Get the address and mail him? Will WMF visit or sue him on behalf of "the Arbitration Committee" until he answers?
  - "The Foundation may need to notify you of receipt of a legal document involving that community member". This sentence totally makes no sense. You == "that community member"? And what a legal document? A legal document calling for "that community member" to be arrested?
- The "destruction process" is also total bogus. A user who no longer has CU/OS access should notify stewards, who then inform the Foundation. First, stewards notice anyway when CU/OS removal happens, because they do it. Second, it reads like the data will only be destroyed if the user "notifies stewards" at all. Can a steward just tell the Foundation sua sponte that someone lost CU/OS or only when the user himself requested it? Third, why stewards at all? They are volunteers, they might also simply forget to impart the "wish for destruction" in a case, etc. If this outrageous proposal succeeds at all, there **needs** to be a qualified WMF staffer who watches Special:Log/rights for removal of CU/OS/steward and is also contactable by users who lose this access, just to be sure, and who sees to it then that the data is really destroyed after the prescribed time. And then not only "in a timely manner following the three (3) year period" but immediately! It is barefaced to say data is stored for maximum 3 years after the loss of access, and then only execute this "in a timely manner" i.e. when we want.

--MF-W 21:57, 14 October 2013 (UTC)

I fully agree with the opinions expressed above me in this section, but I'd like to expand on the problem with giving power to a "user community committee" in this case. There are very, very few projects which have an ArbCom or similar body (and no such body exists at the global level), so these groups shouldn't be included in any policy as the norm. If they are ever mentioned, it should be as an after-note in a different sect)on explaining special cases.

> On this note, the role of a "user community committee" isn't defined at all here. Will they actually have access to scans of ID? It seems to imply that the Foundation is keeping them around so they can look at them later... to contact me or "complete an ongoing case". What does that mean? Can I go to lessthantencontributors.wikipedia.org, become an admin and arbitrator, and then get access to all identified people's documents? Why would an arbitration community, or a "user community committee" even need that sort of information when filling the definition of their role? Google defines arbitration as "The use of an arbitrator to settle a dispute", not "A body who looks at confidentially-submitted IDs and stalks former contributors". Some clarification here would be useful. Ajraddatz (Talk) 23:31, 14 October 2013 (UTC)

- As can be deduced from my contributions, I am a resident of the state of California, so there is no getting around California state law in my case. I can see where this proposal comes from, and I believe there are valid points here. But I believe in some areas that this proposal goes too far. There are several loopholes as mentioned by the others above. I still have yet to go through this in fine detail, but one thing that doesn't strike me too well is the clause saying, in effect, "if you leak private data, we will sue you." Of course, I believe that in some cases legal action may be appropriate, such as a steward/CU willfully violating people's privacy. But the way it's written, it implies that not even our most trusted functionaries are ... trusted, and that honest mistakes will be swiftly and soundly punished by consequences in real life. If that is to be the case, then we might as well have WMF take over all functionary positions, because I don't think there will be many takers for such a *volunteer* role. Functionaries are editors, and their privacy should be protected too. --**Rschen7754** 23:26, 14 October 2013 (UTC)
- I'm also fairly alarmed by this change, on two fronts. **First**, the general idea of the WMF keeping copies of documents of mine that could be used to do everything from open a bank account to getting a duplicate passport is alarming. In the cases of other organizations that have such documents from me, the organizations have track records and demonstrable processes for protecting the data, both physically and electronically (as well as there usually being established legal/governmental processes that hold the organizations to their promised non-disclosure and protection). The WMF, on the other hand, proposes to get these documents from us with a promise of, "We'll totally lock that filing cabinet and password-protect the file!" Unfortunately, organization at the WMF often seems to be lacking, and I simply find myself unable to muster enough confidence in its ability to make this one particular procedure bulletproof, this one time, the first time.

  Second, the idea that they won't disclose my personal information, except when they decide they can disclose it to whoever they want ("permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department") or when they decide it's in their best interest ("needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors"), amounts to "so, we won't give people your passport, except when we will, which might be pretty often, who knows?"

  I was and am perfectly fine with letting someone at the WMF check over my documents to verify my identity (as, indeed, they have already done). But before I'm comfortable with them keeping copies of it for their own purposes, I need to see far, far more detail about a) how my rights (not the WMF's) will be protected as far as who gets copies of my information, and b) how, exactly, my data will be protected. "We'll put a padlock on the cabinet" isn't adequate; I'm looking for something more like "We have designed storage procedure X and had it audited by independent security firm Y, which verifies that this procedure is state-of-the-art and resistant to both tampering and hacking to a level standard in the data-protection industry." The contents of people's passports, identity cards, or driver's licenses isn't the sort of thing you can protect using "agile" development where you start with something that sort of works and then iterate to improve when you find bugs. You need to have proven security from the very first moment, because if this goes wrong, it won't be annoying for the people whose identities are stolen, it will be *catastrophic*. Fluffernutter (talk) 00:29, 15 October 2013 (UTC)
- Man9`good points. On the other hand, WMF has to have some way of knowing who tools holders are (especially CU), and it should be a bit more than WMF staff memory. Perhaps a one-time ID check and registering a name somewhere (plus perhaps other data, such as date of birth, but not full ID scans) would address the concerns above? Pundit (talk) 05:15, 15 October 2013 (UTC)
- I **strongly oppose** this. I echo Snowolf's concerns and with the security breach at Labs, I do not feel comfortable with this change. Echoing what Vituzzu said, I would be one of these users who would leave. Elockid (talk) 22:33, 15 October 2013 (UTC)
- I am in agreement with my colleagues above. Furthermore, I understand why certain contracts mention the possibility of legal action, but these contracts then must include compensation for the signing party. Just like I refuse to sign publication waivers that make me solely responsible before the law if some madman decides to claim my images as his and sue, I feel uncomfortable with the present framework. People who have to answer before the law must know precisely when they are within their purview or not, they must enjoy legal support in case of problem, and they must be paid for the trouble. I am a volunteer here, and while I do pro bono work out of idealism, the pleasure I derive from the very act of contributing is also a factor; having second thoughs about prosecution in the USA for every action I take makes contribution less enjoyable, and there is a point where a contributor, without making a big fuss about it and without necessarly hitting a particular red line, will decide that the boat is overloaded and shrug off their commitment to the projects. Rama (talk) 06:35, 16 October 2013 (UTC)

Explain data retention in the policy itself

I think it would be very helpful for a complete and clear statement from the WMF, within the policy itself, on why identification is necessary and separately why it is necessary to retain hard copies of government-issued identification of volunteers. Many non-US countries have a very different culture when it comes to personal and private information, and are likely to have (and already are having, in some cases) a much stronger negative reaction to this than Americans might overall. It's unfortunate that the policy sort of glosses over the justification for data retention without making a really strong argument in favor of it, so perhaps Geoff and his team can remedy that? **Nathan** T 19:41, 14 October 2013 (UTC)

> Nathan, I know you've already seen this, but to anyone else following this thread, you may be interested in the discussion below regarding why we would like community members with access rights to identify. I'd also like to note that we are open to the possibility of retaining only identifying information about these community members rather than copies of identification documents themselves. We'd love to hear from other community members on this subject. Thanks in advance (and specific thanks to you, Nathan, for your patience as we respond to everyone's input.) Mpaulson (WMF) (talk) 23:18, 31 October 2013 (UTC)

Who needs to identify at all now?

>>Any community member who has been granted access rights and has not previously identified under the previous "Access to nonpublic data" policy (adopted 2007) has sixty (60) days to meet the Identification Requirements of Section 2(b) and the Confidentiality Requirements of Section 2(c) of this Policy."<< Do such users still exist? Afaik nowadays everyone who has access to CU/OS should be listed on IN. --MF-W 22:12, 14 October 2013 (UTC)

If I remember correctly, there might still be some OTRS agents who have not identified to the Foundation, as this was never a requirement that was set in stone. There were some plans to force every OTRS agent to identify to the Foundation in February 2011, but they don't seem to have been put into action, in the end. odder (talk) 22:31, 14 October 2013 (UTC)

When I joined OTRS in September/October 2012 I did not have to identify, though I did a few months later for my OS flag. --**Rschen7754** 23:11, 14 October 2013 (UTC)

Hi MF-W, odder, and Rschen7754. I know that you have seen this related discussion, but I wanted to point out to others who might be following this thread that the OTRS question is still being discussed and we'd love to hear more opinions about whether OTRS members should be included. As for other types of community members who may not have yet identified, this clause is meant to cover anyone who has access rights who may have not known (for whatever reason) that they had to identify under the 2007 policy. Mpaulson (WMF) (talk) 23:37, 31 October 2013 (UTC)

Enwiki ACC

I've notified the enwiki ACC members since this affects us too. Reaper Eternal (talk) 00:46, 15 October 2013 (UTC)

Thank you Reaper, if you want me to send anything out to them please let me know, it was only my list since I was reminded about them but I won't beleaguer the point if not helpful. Jalexander--WMF 02:21, 19 October 2013 (UTC)

WMF?

It's been a few days and other questions have been answered, but not the more concerning questions above. Does the WMF plan to edit the proposal to address these concerns, or should we be making our decision on whether or not to reidentify based on what the proposal is, since the WMF does not plan to address the concerns above? --**Rschen7754** 01:59, 19 October 2013 (UTC)

I would encourage you to wait before making any decisions like that. We want to come up with a good policy that as many as possible are happy with. Michelle has been answering questions from her sick bed at home this week (and I imagine you will see a bit more over the next couple days) but we plan to get together early next week in the office to discuss some of the unanswered questions. The consultation is scheduled to last at least 3 more months (there is no hard deadline, if we're not done then we keep going) exactly so we don't need to rush this. Given the experiences with other policy discussions (ToS/Privacy policy etc) I think we can expect that this is just the start of the discussion and edits (both small and major) to the document(s) in the weeks to come. I will be making sure that I stay on top of the legal team to both strongly think about, and answer, all of the concerns being brought up. Jalexander--WMF 02:20, 19 October 2013 (UTC)

Rschen's concerns are well justified. Over the last few days, Mpaulson has been addressing a lot of minor concerns that don't require pretty much a complete rewrite of the policy, and has even implemented one edit to the policy. At the same time, all of the major concerns have been completely ignored. It just feels like the WMF wants to implement it very close to its current form, and is consequently ignoring any complaints which would require a big change. Thanks for clarifying that these are being looked into and will be addressed... if that's what you're saying. Ajraddatz (Talk) 02:31, 19 October 2013 (UTC)

That is indeed what I am saying :). I know that people are frustrated by a bunch of pieces and we are in no way trying to ignore any of it (I can't think of anything that isn't up for discussion) Jalexander--WMF 02:34, 19 October 2013 (UTC)

I've appreciated the way the largest questions have been thoughtfully addressed. Thanks to the legal team for the thorough and ongoing replies. –SJ talk 21:55, 24 October 2013 (UTC)

Hi Rschen. I just wanted to follow and let you know that we're responding to a lot of the big issues this week. Many of these responses are clarifications and ask for further response from the community. Once we hear from more members of the community on key issues (such as whether we should still be requiring identification at all, submission of identifying information rather than copies of identification documents, what kind of identifying information would be sufficient, what kind of verification of this information would be needed, what would be an acceptable retention period for such information, etc.), we will start making proposed edits based on the feedback. Mpaulson (WMF) (talk) 23:28, 31 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:03, 3 December 2013 (UTC)

Identification

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:05, 3 December 2013 (UTC)***

Would the photo ID have to remain valid for the duration of the time the rights are held? --**Rschen7754** 19:48, 14 October 2013 (UTC)

> Good point. Surely the WMF also needs to be notified on address changes etc. to ensure that all required data is always up-to-date! --MF-W 22:07, 14 October 2013 (UTC)
>
> > Great point, Rschen7754 & MF-W! We will add "inform the Wikimedia Foundation of any change to their name, address, or email address within a reasonable time following such change" to the identification section of the policy draft. We will hold off on addressing the photo ID remaining valid throughout the duration that the rights are held until we hear more input about whether copies of photo identification should be held at all. Thanks! Mpaulson (WMF) (talk) 22:50, 31 October 2013 (UTC)
> >
> > > Lol. I said this as a joke of course, in order to mock the ridiculousness of the proposal. The change (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&diff=6222708&oldid=6222528) of course only adds to the ridiculousness, so you could as well already "address the photo ID remaining valid" while there is finally the option to discuss sth useful like whether copies of photo identification should be held at all. --MF-W 11:59, 8 November 2013 (UTC)

Change of identity information

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:05, 3 December 2013 (UTC)***

What would be done in the event that the identity information of a person changes? I'd like a policy covering the following points:

- For those who currently hold access rights, documentation must be submitted; for those who previously held access rights (and whose information is still retained), documentation may be submitted.
- If a new ID document is submitted, WMF's copy of the old ID document will be discarded; if the submitted documentation of change is not an ID document on its own, both it and the old document will be retained until (if ever) a new ID document is submitted or the retention period expires.
- If a person who previously held access rights submits a new document, this does not reset the retention period.

I'll admit I'm not entirely sold on whether a copy of ID documents should be retained at all, but if it is, a policy on changing information is necessary. (As an aside, is there a reason the name of the policy is being changed from "access to nonpublic data" to "access to nonpublic information"?) MaxHarmony (talk) 21:03, 14 October 2013 (UTC)

> Hi MaxHarmony! These are all excellent points. I will make some proposed edits to the policy draft for your review. As for the name change, it was primarily for consistency. In the new privacy policy draft, the term "information" rather than "data" is used. Thank you for taking the time to make these suggestions. Mpaulson (WMF) (talk) 17:58, 18 October 2013 (UTC)

Valid for Supportteam-members with access to OTRS-queues?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:06, 3 December 2013 (UTC)***

Does the section: *"Community members with access to any tool that permits them to view nonpublic information about other users"* include supportteam members with access to OTRS-queues?

If yes, what is the rationale of requesting to store a copy of the picture ID Documents and residence for Supportteam members. Best regards --Neozoon (talk) 23:16, 14 October 2013 (UTC) (identified member of the German Supportteam)

> Just a note that there is a discussion above here at OTRS_volunteers where Michelle commented and asked for some thoughts. This is something that is currently being discussed internally and having opinions here is very important in my opinion. In general we currently tell people as they join OTRS that they may have to identify (but have not been enforcing that), whether the policies should be merged or not is something I think should be discussed along with this policy as it should be addressed in it (even if it's an exception. Jalexander--WMF 00:25, 16 October 2013 (UTC)

Why a 3-year post removal retention period?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:06, 3 December 2013 (UTC)***

I can see retaining ID information for a period of time, perhaps 6 months to a year after removal (voluntary or involuntary), with a clause stating that information will be retained longer if there is an ongoing internal (WMF/Ombud) investigation; however, three years seems awfully long. I bear in mind the significant number of people with this level of access who are comparatively transient (e.g., students, those whose work requires travel or moving), so three-year-old data is probably fairly useless. Can we have an explanation of where the 3 year period came from? Risker (talk) 23:18, 14 October 2013 (UTC)

Michelle? --MZMcBride (talk) 22:36, 20 October 2013 (UTC)

Hi Risker and MZ. Sorry about the delay. I had pneumonia and am playing a serious game of catch up this week. The reason why we had decided on 3 years is that when discussing potential periods for retention with the Ombudsman Commission, it seemed possible for an investigation concerning the actions of a community member with these kinds of access rights to still be ongoing 2 years after the community member in question had resigned their rights. This could be the case in a particularly complex investigation or one that did not come to the attention of WMF or the Ombudsman Commission until after the community member resigned their rights. That said, I understand that 3 years can be perceived as a long time and if the community believes that investigations of these kinds are all but rarely resolved in a shorter period of time than 3 years, I'm certainly open to hearing what they believe is a more reasonable length of time. Mpaulson (WMF) (talk) 21:34, 22 October 2013 (UTC)

A maximum reasonable time I think would be 6 months after removal, and extended for an investigation as Risker suggests. At the same time, I don't see what benefit holding information for investigations would give anyway, and this gets at the complaint that this change is a solution looking for a problem. Are the functionaries so rogue and out of control and abusing of their rights that this has lead to multiple cases recently where having their personal information on-file would have solved the case, or at least allowed WMF to sue them? If the entire motivation for this change is so that WMF can sue all the crazy rogue functionaries, then all the rhetoric here about us being really trusted people whose input is desirable is just a farce. On the one hand, we're the cream of the crop (or so you'd think reading things like "community members who are in the valuable roles"), but on the other we're so naughty and prone to frivolous revealing of the confidential information we have access to that they need to keep our personal information so they can sue us. I think that before any more responses are given on specifics, the WMF legal team needs to finally answer the question of why this change is happening. Ajraddatz (Talk) 22:23, 22 October 2013 (UTC)

Hi Ajraddatz. Thank you for your input on what you believe to be a reasonable retention period. What do other community members think?
As to your other comments, please see the posting I have done on why we believe a change is needed and the possible solutions that we think we could pursue. We would love to hear your feedback on this issue. We recognize that this is a sensitive topic, but please believe that we are trying in good faith find solutions that work for the community -- and figuring out what's best involves a lot of discussion with the community, which is why we are having this discussion. Mpaulson (WMF) (talk) 22:11, 25 October 2013 (UTC)

I think that's fair. I think someone suggested keeping the real name around for longer due to certain past cases, and I don't have a problem with that either. --**Rschen7754** 22:15, 25 October 2013 (UTC)

There are different answers for me depending on who is holding the records and for what clear purpose. For community investigations, zero, these are legal records I don't see why community bodies, which according to our long history have proven insecure, should hold them, when there can be no legally binding investigation by definition. For the WMF, zero, as again this is a system subject to unspecified future changes or a general loss of corporate memory (refer to many, many cases of private records of all sorts turning up in skips after company changes from wind-up through to office redecorating meaning someone lost track of the filing cabinets). If legal records of identity were held on an escrow contract of some sort, where a leak or data breach means the holder will pay *handsome* compensation out of their data protection insurance (a requirement on Chapters for payment processing as I recall), then perhaps a period of a year might be perfectly reasonable *if* the escrow contract specified the records can only be released as part of a subpoena and the records had to be retained in the country of residence for the person they identify. --Fæ (talk) 23:12, 25 October 2013 (UTC)

sharing info to someone with an nda

The following discussion is closed: ***closing this off for now given the large amount of changes since it was created and the more current discussion about the release to 3rd parties below. Will archive in a couple days unless reopened.***

Perhaps I misumderstand, but I find the following concerning: "*The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department;...*"

Does this mean that the foundation could theoretically give this info to an advertising company provided they signed an nda of some sort? What sort of nda are we talking? As far as I can tell there is no requirement that said nda is a restrictive one, any old nda the foundation legal department likes will do. This seems kind of scary to me.

Good question, Bawolff. We could say instead: "(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department **consistent with the privacy policy**". That would limit transfers for uses set out in the privacy policy, which does not include, for example, advertising. If that works for you, we will make this change. Geoffbrigham (talk) 20:04, 1 November 2013 (UTC)

On the subject of passwords, I'd like something a little stronger than that - encrypted with whatever the current best practise is for crypto, with what specific encryption is used. Is there logging? Do different people use different passwords? How many people have access? Is it stored on a non networked computer? (Perhaps the entire security model is out of scope for this document, but I'd like assurances its not just a dummy password with the file on the hard drive being unencrypted. Bawolff (talk) 02:14, 15 October 2013 (UTC)

> Another good question. Our thinking is to have the same level of security that we might use for electronic employee records. But, to be honest, we will need to research this a bit more once we have an idea on how the community would like to proceed. We offered another alternative below where we would not need to store such information. Thanks for your inquiries! Geoffbrigham (talk) 20:15, 1 November 2013 (UTC)

Some food for thought

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:22, 3 December 2013 (UTC)***

I'd like to offer some food for thought as to what would personally make me comfortable enough to re-submit my id. This is just my personal idea, and others will have different ideas. I feel the wording of the proposal and the way it has been brought about is very disappointing and a bad start, but I think I understand the underlying reasoning, and agree with it to a certain extent.

I first will seek to explain what is so scary about what's currently in the proposal:

- " Physical copies of submitted materials will be kept in locked cabinets designated for this purpose" -- sorry, if I send you a photocopy of my passport, I'd rather not it be in Philippe's locked cabinet. I want it in an actual, serious safe. And I want to know that only Philippe and Geoff have the combination for it.

  > We are open to different security options, including a safe. But I do want to note that a locked cabinet is the same level of security given to the highly sensitive employee material. What do other community members think about the level of security for physical storage?
  > As for who has access, we can limit the people who can access it, but we should avoid naming specific people rather than offices because this policy (if adopted) should ideally apply regardless of whomever holds Geoff or Philippe's role and take into account what happens if both of them are out of the office. Perhaps something along the lines of "access to these materials will be limited to staff members of the Legal and Community Advocacy department of Wikimedia Foundation"? Mpaulson (WMF) (talk) 21:07, 31 October 2013 (UTC)

- "Electronic copies of submitted materials will be protected by passwords or other electronic protections in files designated for this purpose." This part feels like a bad april fools' joke. I send you a scan of my passport, encrypted with PGP and you just stick it in a zip file with a password that anybody can open with Elcomsoft? Please. If you want to retain electronic copies of our IDs, you need it encrypted, in an offline system and audited by reliable third party firms. And again, only Philippe and Geoff can access it.

  > We intend on giving any personal information submitted or held electronically as a result of this policy draft the same level of security that we give to the personal information of WMF employees or our financial information. Mpaulson (WMF) (talk) 22:17, 31 October 2013 (UTC)

- "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." No, if I send my ID, the WMF can only disclose it following a court order, the end.

  > First, I think it's important to note that there are circumstances that would warrant disclosure that are required by law that would not involve a court order. For example, if we receive a legally valid subpoena or warrant, we would be required to comply with it. (Of course, if we had reason to believe that it was not valid, we would challenge it.) This is why we said "required by law" in subsection (B) as opposed to "compelled by a court order".
  > I'd also like to understand why you are opposed to disclosure if a volunteer threatens immediate harm to another person and identifying information is required by the authorities to prevent such harm (covered by subsection (C)). Could you clarify your position? Similarly, I'd like to better understand your objection to subsection (D), which would allow us to disclose information about a volunteer to proper authorities if they, say, purposefully planted any viruses, malware, worms, Trojan horses, or malicious code that could harm our technical infrastructure in violation of the Terms of Use or that could expose the personal, nonpublic information of other users. Mpaulson (WMF) (talk) 21:43, 31 October 2013 (UTC)

- "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." No, if I give you my address, it cannot be disclosed to some random arbitrator from enwiki because they wish to bring a case against me because I don't fill my edit summaries. It should only be used by the WMF's Counsel, after the WMF has been sued because I disclosed confidential informations that damaged a third party to point the judge to me as the person that should be sued. Nothing else, ever.

  > You may be interested in a related discussion addressing this very issue. Mpaulson (WMF) (talk) 21:13, 31 October 2013 (UTC)

- "For this reason, the Wikimedia Foundation retains submitted materials for a period after the community member ceases to have access rights. Submitted materials will be maintained as long as the community member who submitted the materials has access rights, plus up to an additional three (3) years." You do not need 3 years, so you shouldn't have 3 years. 6 months, sure, 3 years, nope, no way.

  We are open to altering the retention period. Would you mind reading the retention period thread and letting us know what period you think would be reasonable in light of what's written there? (I would really appreciate this as I'm trying to move all comments regarding data retention to that thread so that it's easier to track and easier for everyone to see the considerations involved in determining what the data retention period should be.) Thanks in advance! Mpaulson (WMF) (talk) 23:06, 25 October 2013 (UTC)

- "If a community member ceases to have access rights, he or she should notify the Stewards. The Stewards will inform the Wikimedia Foundation and the submitted materials will be destroyed by the Wikimedia Foundation in a timely manner following the three (3) year period." In no way should us, the Stewards, have anything to do with this stuff. Anything that has to do with IDs or related should be handled by WMF personnel trained in the handling of personal data and on a need to know basis. Said personnel should figure out when it should be deleted, not us.

  Please see Philippe's response on this issue below. Thanks! Mpaulson (WMF) (talk) 22:18, 31 October 2013 (UTC)

- "Community members with access rights may submit the required Identification and Confidentiality materials to the Wikimedia Foundation electronically. Hard copies may be submitted on a case-by-case basis." No, it has been long-standing practice to accept ID in the forms most convenient to the user, and this should not stop. Especially given a locked cabinet is better than a zipped and password protected file, which are the options as it stands.

  We would be fine with that change (assuming that identification documents are submitted at all, a decision that is still pending as we are still waiting to hear more from the community on that matter). Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

- But above all, there is no reason for the WMF to keep a copy of my passport. Zero. I understand that you need to know who I am and where I live in case you have to sue me, that is okey. But once you saw my passport and established that I am who I am, you only need to keep this information in your archives, you do not need a copy of my id. Be them encrypted offline archives or locked safes.

  Again, we are interested in hearing from more members of the community on this matter. Would the community be more comfortable if we only retained the identification information rather than copies of the identification documents themselves? Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

- Somebody suggested a bank vault. I actually like that idea. Keep a copy of my name, username and address in a bank vault or if there's a reason why it really can't be there, an outside law firm offices' safe. You don't need anything else.

  We are actually pretty uncomfortable with this possibility. We have some serious concerns about the potential for disclosure if the information is held by third parties. We are pretty vigorous about pushing back on requests for user information when we believe that such requests are not legally valid. We honestly cannot say the same about more traditional institutions such as banks. Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

I know that there are some folks that cannot live with the IDs being retained, or even their name being retained. I respect them, but that is not my case. I am willing to let the WMF have my name even in perpetuity if they wish. I am not willing to let the WMF keep my passport scan in a zipped file or a locker. I think functionaries deserve more than that, and the wording of this proposal is unacceptable, especially given when this was raised before the OTRS community had grave objections to the locker/cabinet. I know you can't win all of the people over on retaining data, but this attempt is not going to win anybody over period as long as it is construed this way. I am still shocked that anybody at the WMF would be so out of touch to think that a locked cabinet or a password-protected archive was anything but a joke. ***Snowolf*** How can I help? 02:38, 15 October 2013 (UTC)

> I would like to highlight my experience of the reality of fraud with regard to passports. *Several years ago an Australian friend was looking for an apartment in Paris, knowing his boyfriend rather well, I acted as his UK reference for a money transaction in London for a deposit of more than 1,000 euros for the lady that was looking to re-let her lease. It was a scam and he lost his money (this is now recognized as a 'classic' scam but it was new back then). With the UK police, I investigated the background and key to the scam was a passport scan that had been doing the rounds with scammers for some time. I managed to contact the lady whos passport it was, and she was the victim of an earlier scam and her identity was being used for multiple later crimes, she put me in touch with a fraud detective in Interpol who was tracking all instances of this fraud. Unfortunately once your ID is compromised this way on the internet, it becomes impossible to put the genii back in the bottle, her scanned passport page (with real name and address details) can be still be found on scam websites and is no doubt still being used to commit fraud in her name.*
> +1 for Snowolf's suggestion that **any ID material is not held by the WMF office, but held in escrow** using a service off-site and only accessed after a direct legal requirement to do so, rather than a request from some unpredictable committee of volunteers who are unlikely to be able to prevent emails or material being "leaked" if it turns out to be of interest to the newspapers. These services range from very cheap to free, from banks and legal firms. --Fæ (talk) 08:20, 15 October 2013 (UTC)
>
> - Good idea, however I can imagine also that some community members could feel LESS safe with a third party involved. Pundit (talk) 06:04, 16 October 2013 (UTC)
>
>   We're still working through some of the points that were raised here, but I'd like to respond to a couple of them: first, regarding having the info held by a third party firm - I think that's a bad idea. If we store it in house, my understanding is that we are, broadly, covered by attorney/client privilege for doc here. (Disclaimer, IANAL).

Stewards - It's been raised that the process as laid out here adds work to the stewards (given that they they have to notify us). I can see the point. I suggest that we remove that line, (*edit: it has been removed.*) and staff will monitor the logged actions for what we need. Philippe (WMF) (talk) 21:59, 25 October 2013 (UTC)

Hi Snowolf. Thank you for your thoughtful comments. We are going to try to address each of your points in turn, in-line. We will get to all of them, but I just wanted to let you know that the responses may come piecemeal because we're trying to address issues throughout the discussion page by subject. Just didn't want you to think that we are only intending to address some of your concerns. Mpaulson (WMF) (talk) 23:01, 25 October 2013 (UTC)

Purpose

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:23, 3 December 2013 (UTC)***

This page, nor the wikimedia-l thread, nor the blog post, say anything about exactly what problem this new policy would solve. The current system works well and I see no reason to change it. I think the new one is going to be purely inconvenient for our existing functionaries, mainly per Snowolf.--Jasper Deng (talk) 04:25, 15 October 2013 (UTC)

I have to agree here. What is the problem with the current system that requires the WMF to give out my address to all and sundry? Chase me ladies, I'm the Cavalry (talk) 13:37, 15 October 2013 (UTC)
Also, just because other sites might do this doesn't mean we should.--Jasper Deng (talk) 04:54, 16 October 2013 (UTC)
I agree as well. There is nothing here that solves a problem. All it does is cause new ones. -Djsasso (talk) 16:43, 21 October 2013 (UTC)

Hi All. You may be interested in reading this post about this very topic. I would be very interested in hearing your thoughts. If you get a chance, please let me know what you think on that discussion thread. Thanks in advance! Mpaulson (WMF) (talk) 22:24, 25 October 2013 (UTC)

Purpose of retention for address

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:24, 3 December 2013 (UTC)***

Thanks for publishing this draft and getting us involved. In particular I think it's good that you've not required that the government-issued identification have your address on it, as some countries like the UK do not have an identity card scheme and as I don't drive my only government-issued photo ID is my passport which doesn't have my address printed on it. However, in spite of me applauding this, it does raise a few questions for me.

1. **Verification of provided address**. It seems that with no way of checking the address that the person provides, there is no way of verifying the address that's given. Is this just an accepted risk you're taking?
2. **Purpose of requesting address**. In light of the fact that the information supplied may be completely fictional, I'm not sure what the purpose of requesting it is. Some clarification may be helpful.

--Deskana (talk) 09:35, 15 October 2013 (UTC)

Some websites, such as couchsurfing, use/used postcards with a code for address verification. If they were accompanied by some wiki merchandise, many users would not mind :) This is apart from the discussion whether an address is actually necessary for the WMF to have. Pundit (talk) 06:02, 16 October 2013 (UTC)

Hmmm..... interesting Jalexander--WMF 02:42, 19 October 2013 (UTC)

Hi Deskana and Pundit! Indeed, these are some great ideas. I would be interested in your thoughts about the general requirement of submitting an address. Mpaulson (WMF) (talk) 20:53, 31 October 2013 (UTC)

What about stolen accounts?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:43, 3 December 2013 (UTC)***

What will happen if one of these "highly-identified" accounts will be stolen? Just some days ago there was a potential security breach when thousands of hashes has been made almost public on WMF labs. So the owner will be legally charged with every misuse of his stolen account? I use quite strong passwords and secure user-side devices/software but still my account can be forced in every other point of the chain bringing me to WMF. So, from an "investigative" point of view, identification via IP will always be needed, so why do we need to store IDs? You should also be aware of the revolution in security measures WMF must to take since another "labs leak" will expose the Foundation to serious legal threats by her own users so I must presume WMF will completely re-design their software and their software development process. My bank and other organisation giving me a legally binding online identities signed strong strong agreement assuring me I won't be charged for their faults nor my good faith faults, will WMF do the same? --Vituzzu (talk) 10:58, 15 October 2013 (UTC)

Yes, this is the point I was trying to make, but you put it more clearly :) --**Rschen7754** 04:25, 16 October 2013 (UTC)

@Mpaulson (WMF): are there plans to clarify the wording (I think it was the confidentiality pledge actually)? Personally I would suggest something like "in cases of willful intent to violate privacy, or gross negligence", but IANAL. --**Rschen7754** 20:11, 30 October 2013 (UTC)

Hello @Rschen7754: and @Vituzzu:, thank you for this question. This policy and the Confidentiality agreement for nonpublic information applies to "you" -- the person using the account. Is there another section where this could be clarified? A user should not share his or her password (under the Terms of use), but it is not a violation of these policies if a user's account is stolen (through no fault of the user). In practice, a user will have his or her technical privileges revoked if it appears that his or her account has been compromised. For example, a steward under the CheckUser policy may remove a checkuser's access. The intent is to ensure that checkuser tools are not used by someone who was not selected and entrusted by the community. Thanks Stephen LaPorte (WMF) (talk) 20:15, 1 November 2013 (UTC)

Board of Trustees

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:44, 3 December 2013 (UTC)***

I'd like to read some words from the Board about this change. --Vituzzu (talk) 11:12, 15 October 2013 (UTC)

On a similar note, has the Ombudsman Commission taken a stand here on this specific proposal? Pundit (talk) 06:06, 16 October 2013 (UTC)

Hi Vituzzu and Pundit! The Board is, of course, welcome and encouraged to join this discussion. And the Ombudsman Commission actually helped us craft the concepts included in this policy draft and provided useful feedback during the drafting process. Mpaulson (WMF) (talk) 23:17, 17 October 2013 (UTC)

That was my understanding, but I wanted this to be clear. Pundit (talk) 06:57, 18 October 2013 (UTC)

Michelle: it's a bit strange to read that the Board is "welcome and encouraged to join this discussion." This policy has no effect unless the Board says so. The Board is quite a bit more than welcome and encouraged to join the discussion... the Board should be actively leading it. --MZMcBride (talk) 22:32, 20 October 2013 (UTC)

Heh. Surprised? Theo10011 (talk) 23:28, 23 October 2013 (UTC)

MZMZ - A global policy such as this would have to be discussed and approved by the Board to take effect. But that does not mean that all public discussion must be led by the Board. LCA in particular is designed to coordinate public discussions about their work, including any policy recommendations they make to the Board -- such as is happening here. In those cases there are reasons not to have the Board jump in with comments before a public discussion, since the hope is to reach an understanding of appropriate community norms, and we are sometimes derailed by threads that try to oppose board and staff comments [rather than empowering the community to draft a policy it finds appropriate in the first place].
The Board has not revisited this policy since 2007 - see also this comment from 2011 when it was last being reinterpreted. Members of the Board are reviewing these policies and proposals at the same time as the rest of the community, thanks to this public discussion; but we don't get to weigh in "as a Board" until there is a recommendation before us. Which, given the quality of the legal-community discussions in recent years, I am certain will be an excellent one. –SJ talk 19:47, 24 October 2013 (UTC)

Vituzzu - the current policy on how users identify to the WMF, and for what reasons, is vague on how identification is implemented. I do think that this should be covered more clearly in an "access to private data" policy -- at least to be clear about current practice. –SJ talk 20:03, 24 October 2013 (UTC)

Michelle - I appreciate your sentiment. It is hard for Board members to join such a discussion individually, since our primary position in these cases is strong support for staff in engaging directly with the community; and since our personal views are often mistaken for Views of the Board. That said, I have shared some brief personal thoughts below, as a community member and not a Board member, in areas where clarification would help me.

Thank you for clarifying, SJ. Your thoughts are always appreciated! Mpaulson (WMF) (talk) 22:20, 24 October 2013 (UTC)

exact scans vs. data

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:45, 3 December 2013 (UTC)***

I understand that WMF may need to be able to link the special trust accounts with actual people. Stewards, checkusers, oversighters have tools which technically allow privacy breaches on all other members of the community and it is only natural, that the safety and privacy of everybody wins with the right to privacy of those tool holders. I'm curious about one thing, though. Several members of the community expressed concern about their ID scans being kept by WMF simply because such IDs, if anything goes wrong, may be used for identity theft. I'm wondering then whether WMF indeed needs full ID scans, or is a basic confirmation of one's identity (with typing a name, date of birth, and possibly a declared or verified address into a database) not a better solution? Pundit (talk) 06:10, 16 October 2013 (UTC)

If the problem here is that we need a legal record of verification, then I would have far fewer concerns in proving my identity to a local notary public (a solicitor on my high street charged me £5 the last time I did this) and then providing the approved relevant scan to an escrow facility in my country (again, these are cheap as chips or even a free service that the WMF bank or regular solicitors could provide). As for the security of a third party, if it is a bank or a solicitor's secure facility, then the level of insurance/compensation available in case of fraud would be far, far higher and more reliable than the WMF can provide. As a solution this reduces risk of fraud for both volunteers and the WMF, or the catastrophic case where volunteers are being forced to sue the WMF for compensation after a disgruntled employee (or someone else hanging around the WMF not-as-secure-as-a-bank offices) does something stupid. --Fæ (talk) 07:11, 16 October 2013 (UTC)

(Btw notary public exists only in Common law)
Actually I contested the whole process of association between accounts and identities since, from a legal point of view, we cannot give any legal warranty about account strength thus an IP check will always be needed. --Vituzzu (talk) 12:34, 16 October 2013 (UTC)

I don't think we're tied to keeping full IDs. We'll have to think on the option some more, to make sure we're not missing something. Would it reduce your other concerns if we did that? Importantly, would you be OK with us asking for things that might not be on all IDs (such as addresses)? -LVilla (WMF) (talk) 22:49, 25 October 2013 (UTC)

Draft confidentiality agreement

The following discussion is closed: ***close, looks like the discussion is finished/stale, will archive in a couple days unless reopened. Jalexander--WMF 22:36, 9 December 2013 (UTC)***

For the record we have a draft of the agreement mentioned up already which is also available for discussion. Jalexander (talk) 23:07, 3 September 2013 (UTC)

So just to begin this part of the discussion, the draft of the agreement says the following: *Authorized Wikimedia community members may include, for example, oversighters, checkusers, functionaries, volunteer developers, and other similar authorized roles.* Can we please clarify what exactly is meant by *functionaries*? Also, including OTRS agents in that list might also be helpful. (I'll try to provide more comments as I read through the text.) odder (talk) 21:41, 19 September 2013 (UTC)

Hi odder! Thank you for your questions and comments! I've responded to each of your inquiries in-line below for the sake of clarity. I hope that's alright.
I agree that the term "functionaries" is a little vague. What we were trying to encompass here was any community member who has been given rights that permit them to access nonpublic, legally sensitive information. However, we realize that different communities may have different terms to describe the group I refer to as "checkusers" or may choose to change the term "checkusers" in the future. Similarly, new roles or access rights may be created in the future by the community that should be covered by this policy, but obviously cannot be explicitly listed. We hoped that the general term "functionaries" would suffice, but we are also very much open to other suggestions.
I also agree that adding OTRS agents to the list of users covered by this policy might be a good idea considering that people who write to OTRS frequently include sensitive information about themselves or others. What do other community members think about this? Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)

I do think that you would risk a lot of people leaving, and would also put those in between the ages of 16-18 in an awkward position... --**Rschen7754** 00:27, 16 October 2013 (UTC)

Hi Michelle, thanks for your answer. I would simply suggest that you remove the word *functionaries* from the draft, as the number of user groups with direct access to non-public, personal and sensitive information is, I believe, very limited; only oversighters, checkusers, stewards and volunteer developers might have access to such information (as well as members of Arbitration Committees on some projects, but they generally hold oversight and/or checkuser rights already). The term *functionaries* is usually supposed to include administrators (and possibly also OTRS agents); you are already using the phrase *and other similar authorized roles*, which, in my feeling, is enough to cover the possible future scenarios you mentioned.

As far as OTRS members are considered, my intention was only to make things more clear to people; if you want to include OTRS agents, then please do so plainly, and we can discuss the pros and cons of the idea afterwards.

As an OTRS agent, I have seen many e-mails which revealed very sensitive personal information about people, such as exact (snail-mail) addresses and phone numbers, not to mention real names or e-mail addresses. I think I can say I've had access to more sensitive personal information as an OTRS agent than as a Commons oversighter — so I can understand why it might be good to include OTRS agents in the list, and have them sign the agreement. However, as Rschen7754 rightly points out, this idea has always been controversial among OTRS agents, and many of them might decide to leave if this requirement is implemented, so I think we should try to discuss it in detail. odder (talk) 10:15, 16 October 2013 (UTC)

What do you think about removing "functionaries" and saying “This policy does not require users whose rights only include the ability to view standard deleted revisions.”? Mpaulson (WMF) (talk) 22:16, 25 October 2013 (UTC)

Sounds good to me; thanks, Michelle! I'm not sure how to address Bawolff's point about #Volunteer developers which was brought with regards to the privacy policy, but which is also relevant for the confidentiality agreement—any ideas? odder (talk) 07:02, 26 October 2013 (UTC)

So I read the draft, and here are some more questions:

Comply with the Privacy Policy; the Access to Nonpublic Information Policy; and any other applicable and nonconflicting community policy relating to nonpublic information; -- the community policy part is quite vague. Moreover, it is my feeling that it complicates this point a bit by mixing the requirements of the WMF and community policies; on a related note, I'm not aware of any community policies concerning non-public information, nor do I think that it should be up to the community to decide that. odder (talk) 21:58, 19 September 2013 (UTC)

The reason why we have included any applicable and nonconflicting community policy relating to nonpublic information is because the Privacy Policy and the Access to Nonpublic Information Policy are baseline protections. Nothing in those policies prevent any particular project's community from creating and enforcing more protective policies with regards to user data. If a community does create such a policy, we would expect community members of that particular project who have special access rights to comply with that community's policies. Does that make sense? Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)

Yes, it does make sense :-) However, we are still left with the question whether the communities should have any say in the subject of protection of user data. So far, this has been a Foundation prerogative, and I wonder if this change would do us any good. (Just throwing a thought.) odder (talk) 10:15, 16 October 2013 (UTC)

The Wikimedia Foundation may pursue available legal remedies. This sounds *very* scary to me, as if the WMF reserved the right to sue me if I violated the agreement. I would very much appreciate a clarification about what's meant by this sentence.

I can understand why this clause sounds scary. Believe me, I hope that we never, ever have to use it. The scenarios that this clause is meant to cover are extreme...for example, if a particular person who has checkuser rights uses those rights to access and copy personal information about users without any good reason and then goes on to publish that information in a inappropriate or malicious way, we would want the ability to legally restrain this person from continuing to publish the private information. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)

Thanks for the clarification, Michelle, it's very helpful. I can definitely understand why you wanted to include this clause in the agreement. odder (talk) 10:15, 16 October 2013 (UTC)

The laws of the State of California and the United States of America will govern this agreement (without reference to conflict of laws principles). This is also very vague; I believe that people should be informed in detail about what applicable laws there are and what are the exact terms that they will agree to if they sign the agreement. (There are many differences between the various jurisdictions our users are located in, and blankly agreeing to be governed by laws you have no idea about is never a good idea, IMHO.) odder (talk) 21:58, 19 September 2013 (UTC)

Actually, the reason why we have this clause is to clear up ambiguity, not to create more. We want to be clear that a particular set of laws will govern the way this agreement is interpreted (in this case, the laws of CA and the US). But I don't think it's reasonable or even possible to provide every law that could apply to any particular situation that could arise in relation to this agreement. It would frankly turn this 1 page or so agreement into a treatise with many, many volumes. For example, the statutory and case law covering contract interpretation alone could fill the better part of a library. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)

Yes, I'm aware of the complexity and the vastness of the U.S. legal code; it wasn't my intention to make you describe any and all laws applicable to this agreement. However, it would still be helpful for many people to know at least the basic terms of the laws they would agree to if they sign the CA. (There are many questions asked about this part by people below, for instance Vituzzu and Fae, so you can see this is something people are actually concerned about.) odder (talk) 10:15, 16 October 2013 (UTC)

Usually there are small differences among the states in the U.S. on issues like construction of the agreement, damages, and consideration (that is, the quid pro quo of contracts). This article (http://docs.law.gwu.edu/facweb/gmaggs/maggs-augsburg.pdf) points out some differences among different states as well as Europe. It is a bit difficult to be more specific because it will depend on the facts of each case to some degree, and, in a common law country, the case law in the jurisdiction. Geoffbrigham (talk) 22:03, 25 October 2013 (UTC)

Thanks for the pointer, Geoff; I'm sure the lecture will be interesting, and I'll try to read more on the subject. odder (talk) 07:02, 26 October 2013 (UTC)

Another part of the agreement got my attention today:

(...) your activity or account may be reviewed by other authorized users or the Wikimedia Foundation.' Does anyone mind explaining the meaning behind *your account (...) may be reviewed* and the meaning of *other authorized users*? I'm especially concerned about a combination of these two parts: *your account may be reviewed by other authorized users*. What does this mean with regards to off-wiki activity such as OTRS? Does this mean that in case of a breach of privacy by a checkuser, other community members with these rights would be able to perform a check on their account? I would welcome an explanation of this point, thanks. odder (talk) 17:50, 7 October 2013 (UTC)

This means that if there is a good reason to suspect that abuse (or mistaken use) has occurred in relation to a particular account with access rights, the Foundation or other community members with the same rights may review the account and its activity to ensure it is in compliance with applicable policies and that nothing has gone wrong. To be honest, it is unlikely that the Foundation would play this kind of role unless the alleged abuse in question was significant. The more likely scenario is that something unusual happens (or something usual happens and was incorrectly documented) and the other users with the same access rights proceed under their own policies to investigate the matter. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)

So, to take your example from above, I'm assuming that in case of a checkuser revealing non-public information about another user off-wiki, other checkusers will be able to perform a check on them — is that right? I'm not exactly sure if volunteer community members should be tasked with ensuring compliance with Foundation's policies in cases like that. Also, I'm assuming that in case of OTRS, it will be the OTRS admins ensuring compliance with the various policies (please correct me if I'm wrong). In any case, thanks so much for your answers, Michelle; I appreciate your time. odder (talk) 10:15, 16 October 2013 (UTC)

The intention here - as I understand it - is to say that nobody gets to do unreviewed actions. Not Checkusers, not oversighters, and not me. It's a bad idea to have a system where anyone can pull data without creating an opportunity for review of the action. That's why we have logs that are automatically created... my read of this sentence is to spell out clearly that if you Checkuser someone, you should expect that the Checkuser logs will be reviewed. Likewise, if you're oversighting, you should expect that those logs are reviewed. That applies to WMF staff too - I review the logs for staff names, and I know that (for instance) when the English Wikipedia sees a staff member do a checkuser who isn't typical, they review it and notify me. So I interpret the sentence to mean that the actions of the accounts may be reviewed (and, as well, other data about the account (ie, was it logged on then?) if needed. Philippe (WMF) (talk) 21:48, 25 October 2013 (UTC)

OTRS volunteers

The following discussion is closed.

The draft is not very clear about identification requirements for regular OTRS volunteers. For some time now (despite many didn't like it), every OTRS volunteer is supposed to be identified, but in practice past volunteers (and perhaps some of the new too) were not asked to provide identification. Is some clarification of the issue coming? --Nemo 06:13, 4 September 2013 (UTC)

Agreed imo. Age restriction for OTRS volunteers is set to 16 currently. In my opinion, OTRS volunteers who do not reached at age 18 should be marked seperately in Identification noticeboard. – Kwj2772 (msg) 08:22, 4 September 2013 (UTC)

That fairly clearly marks someone as "under 18", doesn't it, potentially opening us up to disclosure and child protection issues? Philippe (WMF) (talk) 10:07, 4 September 2013 (UTC)

Then raising the age restriction to 18 would be only option if we're really going to go identification process for OTRS volunteers. Otherwise we can't distinguish them from the identification for checkusers/oversighters. – Kwj2772 (msg) 10:28, 4 September 2013 (UTC)

Couldn't we, though? We just have to do it in a more secure area. For instance, we could use a message board that stewards have access to but others don't. Philippe (WMF) (talk) 10:35, 4 September 2013 (UTC)

Child protection issues for OTRS volunteers?? I might have lost track of what "child protection" term is used for in USA, can you explain? Anyway, whatever you decide please make clear decisions and apply them or it will be again a huge mess with flames everywhere and mass sacrifices of innocents. --Nemo 21:02, 4 September 2013 (UTC)

If an OTRS volunteer is under 18, they deserve the same protection that we offer anyone else. :) Philippe (WMF) (talk) 21:56, 4 September 2013 (UTC)

That is? I just said I've no idea what protection you're talking about... --Nemo 12:29, 5 September 2013 (UTC)

Sounds like protection from revealing personal information, which would happen if you put someone's name in a section which specifies that they are younger than 18 but older than 16. Philippe's logic is definitely sound here, but I wonder if the OTRS age should be raise to 18 for consistency and to address the issues raised. Ajraddatz (Talk) 19:07, 14 October 2013 (UTC)

We have been talking internally about whether OTRS agents should be covered by this policy. Currently, only OTRS administrators are covered. There are strong reasons to consider adding OTRS agents given that they have access to nonpublic emails sent by third parties which frequently include sensitive information about those who sent the email (and others). I understand that the current minimum age for OTRS agents is 16. If we were to add them to this policy, we could either make the minimum age 16 for OTRS agents only and keep the rest at 18 or the OTRS agent minimum age could be raised to 18. What do others think about these ideas? We've love to hear the community's thoughts on this subject. Mpaulson (WMF) (talk) 23:28, 15 October 2013 (UTC)

If you raise the age to 18, then there arises the issue of what to do with those who are between 16 and 18. Any account removals would be publicly logged, and people could guess their age that way. --**Rschen7754** 02:41, 16 October 2013 (UTC)

Fascinating point! If the age is raised, then removing <18 accounts would clearly identify those users as such. However, you couldn't simply grandfather them in - why would the change be needed in the first place if current 16 year olds still had access? Ajraddatz (Talk) 02:54, 16 October 2013 (UTC)

The OTRS admins could simply not remove people <18 from the public list of accounts immediately, but at later times in smaller inconspicuous groups (to make it look like normal fluctuation). --MF-W 14:12, 16 October 2013 (UTC)

Now that you've said that, it's probably not going to be a useful way to hide it. You could just get rid of all non-identified OTRS agents with the same reason, not making public whether it was over their legal ability to usefully identify or not. --Krenair (talk • contribs) 23:53, 20 October 2013 (UTC)

If having <18 people hasn't caused any issues for this long, there won't be any issues for two more years. We could just stop accepting new applications from people under 18, and then people who are currently under 18 will be 18 within two years. -- King of ♥ ♦ ♣ ♠ 23:21, 25 October 2013 (UTC)

Regardless of whether OTRS users should be subjected to this outrageous policy, the thing with the Identification noticeboard needs to be clarified. It is untenable that someone might identify for OTRS, be added to the I.N. and then happen to become a CU/OS/steward based on that entry, even though he is still <18. --MF-W 14:12, 16 October 2013 (UTC)

Yes, but admin actions are generally logged on OTRSwiki. --**Rschen7754** 17:29, 16 October 2013 (UTC)

Speaking as an OTRS volunteer, I have no problem with being identified to this degree - David Gerard (talk) 22:26, 25 October 2013 (UTC)

Doesn't bother me, either. The age issue is interesting, two questions: (1) how many would this affect as of today and (2) is this to do with the age of legal majority and legal responsibility for handling this kind of informaiton (probably covered already but there's a loooot to read through). JzG (talk) 22:54, 25 October 2013 (UTC)

As an OTRS volunteer, I think it would be even necessary to identify yourself, because there are some volunteers that would have probably have much more professional and warm approach to people addressing OTRS, if they weren't allowed to hide behind pseudonyms. And as someone, who became an admin on a local Wikipedia at the age of 14, I don't really think age is a good measure when it comes to someone's maturity, responsibility, loyalty to community or ability of taking autonomous decisions, but in this case it would probably make sense to restrict it to 18 for legal reasons. Of course, the information should stay of a closed nature (at least I don't want that just about everybody has an access to a photocopy of my id and would definitely reconsider my volunteering if any of these data date would become public) --Smihael (talk) 23:48, 25 October 2013 (UTC)

I don't have a problem as well with such identification. I am not sure about the legal issues, but if this wasn't severely needed, I would highly oppose such a restriction. Many of the active Wikimedia contributors are school students, and a lot of them become admins before 18. Possibly many of the OTRS agents, too. The important thing is, how far is this necessary; was there any particular case ever when this caused a serious problem? In the case there wasn't, how much would be the possibility of having such a problem in the future? And what's its worst possible scenario for it? I would like to know what the answers looks like before making an opinion --Abbad (talk) 04:53, 26 October 2013 (UTC).

As volunteer i don't any problem with my identification using a regular system (CU, OS, ...). Alan (talk) 15:16, 26 October 2013 (UTC)

How about no. I gave my real name and my emailadress. This should be enough. I don't see why people have to send ID's. My privacy is worth more than beiing an OTRS-member which I quite enjoy. Some things are private. Why do they want to know what I look like? Why do they want to know where I live? --Natuur12 (talk) 21:02, 26 October 2013 (UTC)

I just wanted to note something, from a personal PoV (although I am an OTRS Admin I am speaking only on behalf of myself). Ever since May 1, 2007 (https://meta.wikimedia.org/w/index.php?title=OTRS/Volunteering&diff=next&oldid=575099), it has been clearly stated on the OTRS Volunteer application page (although over the years there have been minor tweaks to the wording), that applicants *must* be **willing** to provide identification. The current wording is "Before applying, please ensure that you are...Willing to provide identification to the Wikimedia Foundation if necessary, considering the access to nonpublic data policy". *So this really should not be such an issue for OTRS Agents.* Putting that aside, please remember that the current drafted version, and the drafts we've gotten all along up to this point have never included OTRS Agents under the policy; only Administrators will be affected. Rjd0060 (talk) 01:11, 27 October 2013 (UTC)

Thus far "providing identification" has only ever meant that copies of the identification would *not* be retained (something that has been reiterated a number of times since 2007), so I'm afraid I don't see the link. **Thehelpfulone** 01:38, 27 October 2013 (UTC)

There are users that are concerned with providing the ID all together, before even considering the fact that the information will be retained. But again, the most important thing here ... it isn't set to apply to Agents. Just the Admins. Rjd0060 (talk) 01:44, 27 October 2013 (UTC)

What do you folks think about WMF eliminating the identification process and leaving it to the community to come up with their own standards of identification (consistent with the privacy policy)? I have heard so much objection to identification itself or the various proposed means of identification, so I'm interested in your views to this proposal. Identification without retaining the identifying information is not consistent with the spirit of the Board resolution in my opinion ("Only persons *whose identity is known* to the Wikimedia Foundation shall be permitted to have access to any nonpublic data or other nonpublic information....") So I'm honestly thinking of asking the Board to revoke its resolution and leave to the communities to put into place identification processes that work for their specific communities and needs. Thanks for your thoughts. Geoffbrigham (talk) 22:45, 15 November 2013 (UTC)

Balancing WMF's need to protect itself with volunteers' need to protect themselves

I am an OTRS volunteer. Through OTRS I was given access to (i.e. I handled as part of normal OTRS activities) an email in which I was pointed to a file that had enough information easily steal two people's identities. Obviously the file has since been Oversighted.

In order to get access to OTRS I sent a WMF staff member a copy of a state-issued ID, with some information (anything they didn't explicitly ask for) blurred out, with the understanding that the image would be deleted as soon is it was looked at.

I can absolutely understand the WMF's desire to have a better grip on who is handling the sensitive information on WMF projects. While it's certainly not every day that someone uploads a large chunk of personally identifying information to Commons, it's not entirely uncommon either. But it's important to note that all being an OTRS volunteer did was *point me at the file*. The file was already publicly available, and could have been found just as easily by ordinary Commons users doing cleanup (considering that the uploader had a serious misunderstanding of what Commons was, the file was likely uncategorized, and thus someone else finding it while doing cleanup is a near certainty). Hell, it could just as easily have been found by some random editor clicking 'Random file'.

The vast majority of the sensitive information that OTRS volunteers have access to is phone numbers and email addresses. Celebrities generally have paid staff dealing with OTRS on their behalf, so it's really just the phone numbers and email addresses of random, generally unremarkable (no insult intended) people.

The policy, as written, is unpalatable to a majority of the users that are participating in the discussion. That could be because a lot of people read the and policy and did commented because they have no issues, but considering that there are almost no positive messages about the policy, I would have to say that seems unlikely. On the contrary, right now several functionaries that would be effected by the new policy should it go into effect are threatening to resign over several clauses (parts 3.(b) and 3.(d) mostly).

OTRS already has backlogs that come and go based largely on the availability of volunteers, and it needs a large body of people to keep things running smoothly. If this policy is extended to all OTRS members, some of them *will* resign. I personally will, (and although I'm not active now, at one time I was doing a majority of the photosubmissions queue work). I have to imagine that other people will as well. If too many people decide that they're not going to accept the new policy, it leaves OTRS in a weaker position in terms of timeliness of responses, but does it really lead to a stronger position in terms of security? Is there really any positives? Do we really need to have the names and addresses of OTRS volunteers? I don't think so.

The WMF needs to balance the need to protect the WMF with volunteers' need to protect themselves. The WMF wants to have this information on file in case something goes horribly wrong and it becomes a legal issue, either where the WMF has to declare that personal information it was handling was leaked, or where someone writing into OTRS brings legal action (legitimate or no) against the person that responded to them.

However, by the same token, individual users have to protect themselves. Looking at the Wikivoyage fork debacle, one wonders if more people would be parties to that (frivilous) lawsuit if more people's information was public. If the WMF *doesn't have* the names and addresses of volunteers, it can't *give people* that information. That gives volunteers an added layer of protection from, to put it tactfully, are *unpleasant*. If volunteers don't feel that they have that layer of protection, they're not going to be willing to handle the angry people that write in threatening to sue the WMF and everyone that edited some article or another, and they're not going to be willing to handle the people that seem of questionable grounding.

Ultimately, I don't feel that there is enough of a benefit to the WMF, or enough of a risk that the WMF needs to protect against, to warrant having OTRS volunteers as an included body for this policy. Sven Manguard (talk) 20:42, 31 October 2013 (UTC)

> Thanks Sven Manguard. What do you think of our proposal to eliminate the identification process? Geoffbrigham (talk) 00:55, 6 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 18:49, 9 December 2013 (UTC)

Signing the pledge and resulting liability implications

The following discussion is closed: ****Note: Given how the changes made closing this has done, will archive in a couple days unless reopened. Jalexander--WMF 19:12, 9 December 2013 (UTC)***

Having trusted users sign a pledge in association with their full legal identity, appears to be an enforceable contract between the legally identified person and the Wikimedia Foundation. This would appear to make the trusted user liable for damages in a case raised against the WMF for any actions the trusted user may have been involved with, or thought to be involved with, whether they were paid for their time or not. Three questions:

1. By signing this contract, exactly what potential liability does the trusted user take on for the consequences of their actions and is the liability limited or unlimited?

2. Would the WMF be obliged to provide legal identities for trusted users so that a complainant could name them in a legal case of damages?

3. If there is a risk of liability, will the WMF provide liability insurance that will be sufficient to cover expenses or damage claims in any future legal action with respect to any actions a volunteer might have made as a trusted user? I note that in the UK, such insurance is commonplace for charities where volunteers may take on operational duties as well as employees. Wikimedia UK gives its volunteers this form of liability insurance when acting for the charity, and the volunteers have access to the policy to review if they wish.

--Fæ (talk) 23:55, 14 October 2013 (UTC)

> I'm not a lawyer, but I think the question of whether its enforceable or not (and to what extent) is not super settled. I'm sure there is a category of law out there dealing with "contracts" with unpaid volunteers, but I think generally speaking for an agreement to be binding there needs to be a degree of consideration involved. It's a similar issue as applies to non-disclosure agreements between entities where the NDA is the only tie. In this case, the information probably has no commercial value either, so... the agreements are basically a promise to tie you up in court and cost you money with legal fees, that's about it - and even *that* is only for parties within the U.S. Good luck enforcing a non-disclosure agreement against a checkuser in Russia or Italy or China. (edit to add: in other words, its all paper covering the WMF's ass and not much more.) **Nathan** T 00:11, 15 October 2013 (UTC)
>
>> I can understand your concerns, but I'm comfortable with the language of the agreement for our purposes. Consideration usually needs to be only minimal, and frankly resort to enforceability would only be reserved for really exceptional cases; our primary objective is to spell out the clear expectations of the community in the handling of non-public user information, so people comprehend their responsibilities. Courts may limit liability according to the circumstances, but I would imagine that the most common legal remedy would be a declarative judgment to comply with the agreement or injunctive relief not to disclose further private information. I don't understand the question about "legal identities." WMF may be required to disclose information in its possession if it received a legally-valid subpoena consistent with the privacy policy - though we aggressively resist subpoenas that are overly broad or otherwise legally deficient. As a matter of practice, we also notify users when possible relating to subpoenas requesting their user information. See draft privacy policy. Since the volunteers in the community do not act on behalf of WMF, we would not provide insurance, though we do have available for administrators the Legal Fees Assistance Program when applicable. Also we have suggested an alternative approach below that addresses some of the concerns you mention here. Take care. Geoffbrigham (talk) 19:53, 1 November 2013 (UTC)
>>
>>> @Geoffbrigham: Well, the problem is that a lot of volunteers are not comfortable with the language. Our signing this pledge would basically give our legally binding consent for the WMF to file a suit against us for damages. I've interacted with enough WMFers to know that you would only pursue legal action when necessary; however, we don't know who the WMF will hire down the road, and we would hate to be wrong about something like this. Adding additional language to clarify the scenarios in which WMF would file a suit would go a long way. Speaking for myself, this is the dealbreaker for me - I might not be happy about the rest of it, but I might go along with it anyway; yet the liability issue and my possibly having to take out insurance just to be a steward/CU/OS or whatever is problematic. --**Rschen7754** 20:17, 1 November 2013 (UTC)
>>>
>>>> Thanks for the clarifications Geoff. I take from your statement that:

1. Despite insurance being mentioned elsewhere on this talk page, the WMF does not actually insure any volunteers or other trusted users and has no intention of doing so, even where WMF projects rely on these volunteered services. I note that some Chapters do insure volunteers when acting in roles that would otherwise have to happen through paid project contractors, and this does happen as standard good practice for a large proportion of other charities that rely on volunteers to deliver charitable services to their beneficiaries.
2. You understand my concerns, but you remain comfortable with the policy as it fits your purposes.
3. The legal document has the primary objective of spelling out expectations for handing non-public user information. That it now creates a mechanism for legal enforcement, such as a volunteer being sued by the WMF for indefinite sums of money, seems a secondary concern.
4. The WMF shall pass on legal identities of volunteers in response to any valid subpoena from any party.

--Fæ (talk) 23:34, 1 November 2013 (UTC)

Hi Rschen - so I guess I need to understand better what you think is acceptable. As we suggested above, we could create a regime without identification, which would alleviate some of the above concerns. If that is not the approach that the community wants, we could try to limit the type of legal relief - such as a restriction to injunctive relief. Or we could allow monetary damages up to a certain amount ($30,000?) or only with a significant level of legal intent (something like "willful" disclosure). The challenge is that we cannot anticipate all situations. The one "test" question I ask myself is if a checkuser sells nonpublic information for personal profit, what remedies would the community find appropriate? I would be most interested in your thoughts on this. Thanks. Geoffbrigham (talk) 08:55, 6 November 2013 (UTC)

"Willful disclosure" would be fine by me, or "gross negligence" (choosing a password like "password" for example, or allowing someone to borrow your steward account and that person does bad things with it, etc... when the holder of the advanced rights clearly should know better - though I can see how that might be a harder line to draw). I personally don't see the same issues with injunctive relief, since at least according to my understanding, any financial impact would be minimal (as long as you don't break the agreement). I don't think many people would have problems with the WMF asking for monetary damages if someone with access to public data purposefully violated someone's privacy to the extent that it caused them real-life consequences (though the case could be made for the person who was outed suing too...) --**Rschen7754** 09:13, 6 November 2013 (UTC)

Rschen - You are correct that injunctive relief would be limited to an order to stop doing something (like "stop your access to and distribution of nonpublic information") - without monetary damage awards. We could limit monetary damages to "gross negligence and willful disclosure." It would mean that a volunteer acting negligently with real consequences to the privacy of others would not pay monetary damages pursuant to the agreement. Does that work for you (and others)? Geoffbrigham (talk) 23:59, 6 November 2013 (UTC)

Hi Geoff, you have used some words that I find difficult to interpret, both due to my past professional experience and probably because I am reading them with a UK understanding of English whilst you are writing them from a USA standard. To be honest I worry that many readers here might jump to incorrect interpretations of the specific legal words you are using and so their feedback might end up being based on unwarranted assumptions.
Putting aside "willful disclosure" (though I think that needs specifying), my understanding of a statement that the WMF will *"limit future claims of damages against volunteers to cases of gross negligence"* is linguistically and legally equivalent to the WMF will *"be free to claim (unlimited) damages against any volunteer where there are allegations of them behaving carelessly"*. It might help our understanding if you could explain your understanding of the specific scenarios that "gross negligence" or carelessness can apply to, in the context of Wikimedia volunteer activities, in plain English, that volunteers can then use as a reference to go back to, in the unlikely event of this becoming a reality. My apologies if I am misunderstanding your intended meanings here, though if I am having difficulty, I am certain others are too. Thanks --Fæ (talk) 00:21, 7 November 2013 (UTC)
I guess I'm not sure what the difference between "gross negligence" and "negligence" is - is there an accepted legal definition? Other than that, I personally am fine with it. --**Rschen7754** 00:36, 7 November 2013 (UTC)

Good question Rschen. The difference between negligence and gross negligence will depend on the facts and the duty of care that someone exercises. Some helpful references are here on negligence and gross negligence. Geoffbrigham (talk) 01:10, 7 November 2013 (UTC)

Thanks for the clarification Geoff. The English Wikipedia article you provide for a legal definition appears to show that the difference between negligence and gross negligence is a matter of debate and as clear as mud. I suggest if the WMF wishes to have a legally enforceable policy and if anything goes wrong in the future it can be shown that volunteers accused of carelessness were clearly advised of the policy/pledge and its consequences in a way they could be judged to understand, then the WMF will have to define these terms in specific and appropriate ways that us volunteers do understand.

For example, as a Wikimedia OTRS volunteer the WMF has now stated that I have no legal protection or insurance, effectively if anything goes wrong then my house is at risk. If I agree to the pledge, does this mean that the WMF will help those that wish to sue me or that the WMF will sue me for damages themselves, say for carelessly pressing the send button on an email thread with personal or legal information in it, after putting in the wrong email address?

It would be really nice if at some point the WMF were to turn this around and put our minds to rest by offering liability insurance for unpaid volunteers that were taking on these functions for Wikimedia, in the same way employees were protected. This already happens in Chapters and other charities, it seems odd that the WMF is resisting this solution. --Fæ (talk) 09:11, 7 November 2013 (UTC)

@Geoffbrigham: Having thought on this, I do wonder if adding "gross negligence" is opening up a can of worms, and maybe it should be left as "willful intent". "Willful intent" seems to be closer to the practice that I have heard from another staff member, as to their thoughts when they would pursue legal action (for extreme cases of someone revealing massive amounts of personal information). --**Rschen7754** 10:53, 15 November 2013 (UTC)

Hi Rschen7754 - Let's see what others say, but personally I'm fine with limiting statuary damages to acts of willful intent. Geoffbrigham (talk) 01:26, 16 November 2013 (UTC)

Hi Geoff, I am glad to see some movement on the odd word. A pity that the larger direct questions are seen to go unanswered. --Fæ (talk) 03:48, 16 November 2013 (UTC)

Bump. --**Rschen7754** 20:58, 3 December 2013 (UTC)

Just a note that I've poked the lawyers for this thread. Jalexander--WMF 21:10, 3 December 2013 (UTC)

OK ... let's limit it to willful intent, given no other responses here. I will ask James to make the change. Geoffbrigham (talk) 21:36, 3 December 2013 (UTC)

Consideration of feedback given over the past week

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:13, 9 December 2013 (UTC)***

I would like to thank all of you who have provided very thoughtful feedback on this policy draft over the past week. Your suggestions and questions are much appreciated and have given us a lot to think about. We are internally discussing and brainstorming about many of the issues you have raised and I hope to provide more detailed responses and alternative suggestions over the next week. We may not get to everyone's comments as quickly as we hope to, but please be assured that we are reading and thinking about what each of you say in this discussion and will respond as best as we are able. Thank you again for taking the time to help shape and improve this policy draft. We sincerely hope that with the input we receive over the next few months, we will be able to craft a policy that reflects community values and adequately protects the privacy of both the community members who are in the valuable roles affected by this policy as well as the users whose nonpublic information they handle. Mpaulson (WMF) (talk) 17:24, 20 October 2013 (UTC)

Affected users who will resign if the policy is implemented in its current shape

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. It seems if we're going to have a list like this it should start anew given the large changes. Jalexander--WMF 19:19, 9 December 2013 (UTC)***

(this one (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&oldid=6088605), where only non-central feedback was yet taken into consideration)

1. MF-W (steward, OTRS access) 22:04, 20 October 2013 (UTC)

I haven't had time to read through your comments above quite yet, but it seems strange that nobody is editing the proposed policy to make it acceptable. It's a draft. Be bold! --MZMcBride (talk) 22:34, 20 October 2013 (UTC)

I think one of the main issues is that there is no specified/apparent reason for this change. It's a solution looking for a problem. It doesn't make sense to try and fix parts of it when the reason behind the entire thing is one of the biggest issues. Ajraddatz (Talk) 22:52, 20 October 2013 (UTC)

Do you agree with having wmf:access to nonpublic information policy? --MZMcBride (talk) 02:01, 21 October 2013 (UTC)

Your reply addresses nothing of what I said. I agreed to that policy when I identified to the foundation. You'll notice that I specify the need for change which is lacking, not the need for the policy in the first place. Ajraddatz (Talk) 02:11, 21 October 2013 (UTC)

Sorry, when you said "it's a solution looking for a problem," I thought you might mean having this policy was a solution looking for a problem, not updating it. I've attempted a better system of discussion below, though I understand that you feel a rewrite is entirely unnecessary. --MZMcBride (talk) 02:54, 21 October 2013 (UTC)

Ah. Sorry for my hostile response too, I assumed bad faith and thought you were trying to lead my logic to somewhere that I didn't want it to go. I've been studying Plato's works too much recently :/ Ajraddatz (Talk) 03:18, 21 October 2013 (UTC)

2. Trijnstel talk (steward, CU commons, CU meta, OTRS access) 22:17, 20 October 2013 (UTC) Unless some major changes are made ... otherwise I'm not sure I would stay.

   What kind of major changes? --MZMcBride (talk) 22:34, 20 October 2013 (UTC)

   I do not wish to re-identify so that the WMF can keep my ID. That change should be reverted (among others). Trijnstel talk 16:15, 21 October 2013 (UTC)

3. **Rschen7754** 22:28, 20 October 2013 (UTC) (Wikidata oversighter, OTRS access) Only because I have no money to give to the WMF if they sue me for an honest mistake.

   Noting that if the proposal as written passed as of this timestamp, I would be able to fulfill the requirements. --**Rschen7754** 10:47, 4 December 2013 (UTC)

4. Vituzzu (talk) (steward, OTRS access, meta checkuser) it should completely rewritten following a bottom-up process. 22:35, 20 October 2013 (UTC)
5. User:Nillerdk (OTRS access): I will not accept WMF to give away my ID to any third party, not even if required by US law. I will thus not give WMF in USA my personal informations under any circumstances. I *would* give personal informations to my local chapter, but I would only allow them to share my ID with third parties if required by national low in my country. Nillerdk (talk) 15:55, 21 October 2013 (UTC)
6. -**Barras talk** (steward, meta CU, meta OS, simpleWP OS, simpleWP CU, OTRS, CU-l admin if that matters, and while I'm on it probably just all rights straight away as protest, which includes several admin and crat rights along with my duties as GC for both groups, wikimedia/wikipedia and cvn) - As I'm not allowed by German law to re-identify under the condition, that WMF retains a copy of my ID card. See German laws §§14-20 PAuswG. I won't break German law to fulfill some weird rule here. -**Barras talk** 15:57, 21 October 2013 (UTC)
7. I probably would as well. I don't need these rights. So subjecting myself to such a potentially damaging situation is probably not in my future. -Djsasso (talk) 17:05, 21 October 2013 (UTC)
8. DaB. (talk) (OTRS-access, dewp-ml-admin, Toolserver-admin (until end of year) and I'm sure some more). The WMF is not able to protect such simple things as email-addresses or password-hashes, so I can not trust them with something as valuable as my passport. That the US is a 3th world-country in terms of Datenschutz is another problem. And finally I'm not allowed by German law to make a copy and give it to the WMF. --DaB. (talk) 19:21, 21 October 2013 (UTC)
9. Should the policy be adopted in its current state, I would have no choice but to let my identification lapse and hence be removed as steward and enwiki oversighter. While I truly enjoy the work we do here, and would love to keep doing it, the policy as it's worded is not acceptable, it's amateurish and it's stupid. It shows how little somebody at the WMF cares about our personal info, and does not make me sure enough that my information will be safe. I am more than willing to accept some compromise, but this is a scorched earth policy and it hurts me to see the WMF take this approach. We are volunteers, we built this projects or helped maintain them, we don't deserve to be treated like this. ***Snowolf*** How can I help? 16:57, 22 October 2013 (UTC)
10. The WMF can not be trusted bacause it is based in the US. It's that simple and I will resign my OTRS-access as soon as I am prompted to send a copy of my ID card. --McZusatz (talk) 14:53, 24 October 2013 (UTC)
11. --Natuur12 (talk) 21:10, 26 October 2013 (UTC) I will quite as an OTRS-voluntere if this policy becomes real.

Hi All. First, I would like to note that nothing in this policy draft is settled. The draft is just that...a draft. Anything contained within it is up for debate and suggestions. Second, we would really like to hear your thoughts on the discussion below about whether an identification policy is still needed. Thank you all in advance for your feedback. Mpaulson (WMF) (talk) 22:39, 24 October 2013 (UTC)

Volunteer developers

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:20, 9 December 2013 (UTC)***

There are some very weird ideas that a lot of people appear to hold about what/who the developers are. Some people think that we're all paid WMF staff. Others think that we're all system administrators. Those that think we're all system administrators probably think that we can all see nonpublic information. This document arguably makes that assumption or implication in a couple of places:

> "The following conditions are minimum requirements that all community members, including volunteer developers, must meet to qualify as a candidate."
> "All community members who are granted access to nonpublic information rights ("access rights"), except volunteer developers, are typically chosen by the community"

Volunteer developers are not automatically granted access to any nonpublic information. It's unclear to me whether or not this policy could cause any issues, but still... --Krenair (talk • contribs) 22:43, 20 October 2013 (UTC)

A fine point, Krenair. "Volunteer sysadmins and others with access to shared databases" might be more appropriate here. –SJ talk 19:40, 24 October 2013 (UTC)

Hi Krenair and SJ! This policy draft was meant to only cover volunteer developers who do have access to nonpublic information, not every volunteer developer. SJ, is there any risk with your suggested wording that it would inadvertently cover developers who only have access to shared databases that do not include nonpublic information? Mpaulson (WMF) (talk) 22:45, 24 October 2013 (UTC)

The language you use the first time it comes up in this document is good. –SJ talk 05:13, 25 October 2013 (UTC)

Policy should be rejected!

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:22, 9 December 2013 (UTC)***

This is far beyond what is actually needed for the Wikimedia movement. I am feeling very uncomfortable if the WMF even thinks about this too far going proposal. After all the NSA/etc scandals this is what they come up with?? Sorry, absolutely no. In the whole text I see no reasonable explanation why extra requirements for identification are needed. A lot of bla bla but no actual reason why there is an actual need for. "*Because we believe that safeguarding the privacy of the Wikimedia community is an important Wikimedia value,*" -> if WMF is really thinking that, they wouldn't have proposed this policy that asks too much of giving up the privacy of volunteers. Romaine (talk) 01:12, 21 October 2013 (UTC)

Identity fraud is one of the most intrusive things people can experience. Identity fraud starts often with people knowing the birth date, as that information is often used for organisations to identify someone over the fone (etc). The WMF has no reason at all to keep copies/scans of an ID card. The government in the Netherlands forbids making copies/scans of IDs and also highly recommends not to disclose any information on the ID cards to unauthorized people. WMF is in the private sector and is not authorized to ask for this. Romaine (talk) 01:42, 29 October 2013 (UTC)

Hi Romaine. I just wanted to make sure you saw the more detailed reasoning laid out in the discussion below. I also wanted to make it clear that we are very open to alternate ideas about how community members with access rights identify to WMF and are interested in hearing your ideas. Mpaulson (WMF) (talk) 18:34, 31 October 2013 (UTC)

Attempt at a better evaluation of this draft

The following discussion is closed: ***Closing this whole section because it's all based on the old draft, including the quotes etc, and there hasn't been much response on it for a while partially because of that. Will archive in a couple days unless there is a reason to keep it open. Jalexander--WMF 20:14, 9 December 2013 (UTC)***

I'm going to try subsections and a cute template ({{talk page section}}) to evaluate each section of this proposed rewrite to wmf:Access to nonpublic data policy. I'm going to try to do this in a logical order. --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

I am having difficulty of understanding the value of eating up volunteer time to create a detailed section by section or word by word review, when fundamental questions such as why this policy is needed, what the legal impact on unpaid volunteers is going to be and who will be given access to critical legal records of identity, have yet to be answered. The detailed text of the policy draft is likely to be significantly changed or have different assumptions underpinning it before these questions are resolved. Thanks --Fæ (talk) 13:06, 21 October 2013 (UTC)

The very first subsection covers the "why this policy is needed" needed question, doesn't it? Part of finding consensus is identifying areas of disagreement. We currently have a similar policy passed by the Board in 2007. Do you disagree with having this policy? If not, we should then discuss the proposed rewrite. If nobody agrees with any of the sections of the proposed rewrite, it'll be fairly trivial to reject the entire rewrite outright, right? --MZMcBride (talk) 13:17, 21 October 2013 (UTC)

No, it does not, this was raised earlier on this page and is still awaiting an answer. You cannot start a detailed document review, paragraph by paragraph, until the underpinning reasons for why the document exists and what impact enforcing it will have, is addressed. As to whether I disagree with this document or not may actually be irrelevant, the WMF are not legally bound to respect a community consensus here, and unless I missed it somewhere, I do not think they have stated anywhere that they shall respect a consensus as a management choice. --Fæ (talk) 13:40, 21 October 2013 (UTC)

+1. It certainly makes sense to write down comments section by section or piece by criticized piece, but this has already been done above by some users, see e.g. #Some food for thought by Snowolf. Comments are piling up on this page for about a week now, in which people protest against all sorts of sentences which they perceive as very objectionable in the draft. Meanwhile the Foundation hardly reacts. It is nice to read in #Consideration of feedback given over the past week that WMF discusses what we write and will at some time maybe react (hahaha), and that M. Paulson has even been answering here while being sick (which is, no doubt, sth. we can be grateful for), but afaik WMF has numerous people, also in its "Legal team", which surely is at fault for this draft, and it would be quite nice if they could at least devote the same time to discussing here as we volunteers do. Yesterday I was asked whether I hadn't commented at #Purpose 2 (a section whose content I agree with) yet - quite simply, I have already said what is expressed there in a different section on this page or on the checkuser-l list or on IRC (where also WMF staffers were present / able to read it). To sum up, I see all the same concerns being had by multiple people and being mentioned again and again, yet WMF is more or less silent. So I don't really have any motivation to contribute to such a systematical analysis of the proposal, when I see no reaction to comments anyway. --MF-W 14:35, 21 October 2013 (UTC)

I don't think it's entirely fair to treat the legal team as if they're ignoring us because they don't have immediate answers. Remember, these are people with (for the most part) regular 9-5 daily jobs, who are trying to tick the boxes that they feel need to be ticked before they can present any proposal to us. When Michelle says they are discussing our feedback, I tend to think they're doing just that - discussing our feedback and trying to figure out how to integrate it with whatever it is they feel the policy needs to accomplish, per whatever WMF reasoning underlays that need (which, yes, it would be nice if they could get around to explaining that part to us). I don't think there's any doubt that they now understand just how vehemently people oppose the proposal as it's written (and there's no reason people can't keep sharing their opinions on the current proposal while we wait for a response), but these are lawyers, who need to get their wording bulletproof before they send it out into the world. If we're not willing to wait for them to have a coherent response, the other option is a handful of legal team members chaotically attempting to share what they personally think might happen once a new proposal is offered, followed by them having to backtrack once things change a little, and an end result much like some of the less pleasant software deployments we've had lately where no one knows exactly what "the response" is and everyone's reacting to something different. Rather than going down that rabbit hole, let's give Michelle, Geoff, and team a reasonable chance to respond in detail (in business-day time, not constant-wiki time) before we start assuming that they have no intention of working with us. Fluffernutter (talk) 15:31, 21 October 2013 (UTC)

Fæ: Re: "not legally bound to respect a community consensus here," you seem to be a bit confused about how policies like this are enacted. The Wikimedia Foundation legal team can certainly propose rewrites and can advocate for changes to this policy, however the Board decides. wmf:Access to nonpublic data policy is the current policy and nothing that the legal team does can undermine this. Whether the Board itself is strictly bound to follow community consensus is a tricky question. :-) In this particular case, we seem to have the bold (rewrite) and plenty of discussion, but little editing, which is worrying and against the typical BRD process. If there are problematic parts of this rewrite, let's figure out what those are and address them on-wiki. I think certain pieces of this rewrite are completely uncontroversial. Those pieces, at least, should be simple enough to resolve/approve before we get to the more difficult and contentious pieces. --MZMcBride (talk) 16:26, 21 October 2013 (UTC)

Thanks for your concern that I might be confused. However I believe that your assertions that the WMF board of trustees (a partially elected body) overrules a Wikimedia community consensus, and that this WMF legal document can be changed by using the practices used on the English Wikipedia for writing encyclopaedia articles are not terribly helpful. --Fæ (talk) 19:22, 21 October 2013 (UTC)

If it helps, BRD is also documented locally. :-) This isn't a legal document and it's strange that you would suggest that it is. This document is a proposed rewrite to a standing Board-approved policy. Regarding supremacy, the Board is indisputably the ultimate arbiter (cf. wmf:Bylaws).
I have considerable experience in meta-matters and I'm trying to help move the discussion forward. Unfortunately, I'm not sure the same can be currently said of you. --MZMcBride (talk) 20:17, 21 October 2013 (UTC)

I'm obviously unwelcome and you seem determined to make this discussion unpleasant and personal, so I'll not bother contributing further. Good luck with it. --Fæ (talk) 20:42, 21 October 2013 (UTC)

Policy itself

Status: In discussion

We currently have wmf:Access to nonpublic data policy, passed by the Board in 2007. Does anyone think Wikimedia should *not* have this policy any longer (i.e., the Board should get rid of this policy)? I believe there's general consensus to continue having this policy in some form, but before we go any further, we should make sure. :-) --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

- It seems reasonable to have a policy. --MZMcBride (talk) 02:47, 21 October 2013 (UTC)
- So it does. –SJ talk 20:33, 24 October 2013 (UTC)
- There should be a policy about it and access to nonpublic data needs to be restricted, imo. -**Barras talk** 09:35, 26 October 2013 (UTC)

Title

Status: In discussion

Assuming you agree with having a policy of this nature, we can start at the top. There's a discrepancy between this page's title ("Access to nonpublic information policy") and the policy from 2007 ("Access to nonpublic *data* policy"). Should the title be changed? Should this page be moved? Thoughts? --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

- The titles should be synchronized. I don't really care which is chosen. --MZMcBride (talk) 02:54, 21 October 2013 (UTC)
- Synchrony improves harmony. –SJ talk 20:33, 24 October 2013 (UTC)
- If this policy draft is adopted by the Board, there will only be one title (Access to Nonpublic Information Policy) because it would be replacing the current policy, so it will be synchronized. The reason why I changed it to "information" rather than "data" was to be consistent with the privacy policy draft which refers to things like "personal information" rather than "personal data" and I thought consistency between the two policy drafts would be helpful in that regard. Mpaulson (WMF) (talk) 22:45, 30 October 2013 (UTC)

User-friendly summary

Status: In discussion

There's a "user-friendly summary" at the top of the page:

Text of user-friendly summary [show]

Is it necessary to include a summary with this document? Does anyone agree or disagree with including this summary? (Please focus only on the summary's inclusion itself, the content itself will be discussed below.)

- I'm not sure a summary is needed here. --MZMcBride (talk) 02:48, 21 October 2013 (UTC)
- I find it useful but perhaps it could be briefer; I worry at the first list for instance, as it may be interpreted as comprehensive. –SJ talk 20:33, 24 October 2013 (UTC)
- We have generally received a lot of positive feedback about the user-friendly summaries. While I personally like reading through entire policies, I completely understand that most people are not like me in that regard. We hope that the user-friendly summary will alert people to the most important parts of the policy and allow them to easily find and read the details of the sections that are the important to them. We try to alert readers to the fact that the summary is not comprehensive with the disclaimer on top stating "Disclaimer: This summary is not a part of the Access to Nonpublic Information Policy and is not a legal document. It is simply a handy reference for understanding the full Access to Nonpublic Information Policy. Think of it as the user-friendly interface." Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Purpose paragraph 1

Status: In discussion

Purpose paragraph 1 [show]

Does anyone agree or disagree with any part of this section?

- There's a semicolon splice ("content on the Sites;"). The final sentence doesn't make any sense. It says "Certain community members are entrusted with access to limited amounts of nonpublic information regarding others users, such as ...", but an example of limited nonpublic information isn't given. Instead, it tries to describe sockpuppeting to an outsider. This is a pretty strange sentence. --MZMcBride (talk) 02:51, 21 October 2013 (UTC)
- Thank you for pointing this out, MZ. As to your first concern, do you believe a comma would be more appropriate than a semicolon? As to your second concern, does this work better: To manage this immense task effectively, certain community members are entrusted with access to limited amounts of nonpublic information regarding other users. For example, a trusted community member who has "checkuser" rights could use those rights to investigate whether a single user is using multiple accounts in a manner inconsistent with Wikimedia policies. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Purpose paragraph 2

Status: In discussion

Purpose paragraph 2 [show]

Does anyone agree or disagree with any part of this section?

Scope paragraph 1

Status: In discussion

Scope paragraph 1 [show]

Does anyone agree or disagree with any part of this section?

- Does the "volunteer developer to access to nonpublic information" mean all Toolserver users? --MZMcBride (talk) 02:55, 21 October 2013 (UTC)
  - It's Labs now. --**Rschen7754** 18:53, 21 October 2013 (UTC)
    - Hi Rschen7754. Err, yes, I'm familiar with Wikimedia Labs. However, Toolserver users have access to the archive table and partial access to the user_properties and watchlist tables, among others. These database tables contain non-public information, which is why I asked the question I asked. --MZMcBride (talk) 20:19, 21 October 2013 (UTC)
- Does this include OTRS members? As we all know there is a major difference between stewards, checkusers & oversighters who have special access to the wikis and OTRS members who access correspondence that is separate from the wikis and where people know that their emails will be read by volunteers. I ask because it is worded *to view nonpublic information about other users*. OTRS members have access to nonpublic information but the term *users* usually refers to accounts on wikis which is possibly different from the clients send emails to the OTRS addresses. A significant part of the OTRS correspondence comes from people who never signed up as a user on any of our wikis. --AFBorchert (talk) 18:10, 22 October 2013 (UTC)

  This is worth specifying explicitly, as has been done in the past. –SJ talk 20:33, 24 October 2013 (UTC)

- MZ - This policy draft is intended to apply to Labs & Toolserver users who are granted access to nonpublic information. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- AFBorchert - This policy draft currently only includes OTRS administrators, but we really would appreciate input from the community in the discussion above about whether it should also apply to OTRS agents. I agree that there is some ambiguity due to the term "users". I think if OTRS agents were to be included, we would change that to something along the lines of "view nonpublic information about other users or nonpublic information submitted through OTRS". I am open to alternate wording suggestions though. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Scope paragraph 2

Status: In discussion

Scope paragraph 2	[show]

Does anyone agree or disagree with any part of this section?

- "Election committee" is too unspecific. Nobody knows which one. --MF-W 14:24, 21 October 2013 (UTC)
  - Hmm, I agree. And broadly, how is the determination made as to whether this policy is applicable to a specific group? --MZMcBride (talk) 01:25, 22 October 2013 (UTC)
- Hm... are OTRS administrators included but not other OTRS members? I would suggest not to enumerate some samples but try to give a precise definition (see above) and/or try to enumerate all groups to which this applies now (with possible more coming). --AFBorchert (talk) 18:13, 22 October 2013 (UTC)

  I agree with the value in a precise definition. That also helps clarify why this policy exists in the first place. However a list of all affected groups should not be too long, and makes a useful supplement. –SJ talk 20:33, 24 October 2013 (UTC)

- The groups listed there are only meant to serve as examples. The more specific scope is defined earlier by what the individuals can do -- "Community members with access to any tool that permits them to view nonpublic information about other users (such as the CheckUser tool);Community members with the ability to access content or user information which has been removed from administrator view (such as the Suppression tool); and Volunteer developers with access to nonpublic information." I would not be opposed to listing more examples of groups (or even all of the groups we can think of that currently fall into these categories, but I'm hesitant to make an exclusive list because new groups could form, those groups could change names, and sometimes there may be certain people within a group that need to identify (because they have access to nonpublic info) while other people in that group do not (because they only have access to public info). Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements intro paragraph

Status: In discussion

Requirements paragraph 1	[show]

Does anyone agree or disagree with any part of this section?

- Please note that OTRS members and OTRS administrators are not chosen by the community of contributers. The question is if this point really needs to be elaborated here. I think it is best to remove this section. --AFBorchert (talk) 18:18, 22 October 2013 (UTC)
- I agree that "All... are typically chosen" may not be clear. The whole section could be reworded to focus on the requirements needed to get access to nonpublic data; rather than framing them as requirements for any particular selection process. –SJ talk 20:33, 24 October 2013 (UTC)
- That's a good point, AFBorchert. SJ - the reason why we included this section was to point out to more inexperienced users that the community members who have these access rights are trusted members of the community who have been vetted by the community. Do either of you have any suggestions as to how we could improve the wording in this section? Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

  How about this: *The following conditions are requirements that all community members should meet before being granted access to n.p.i.r. ("access rights"). These should also be considered requirements to be a candidate for any community-run selection process for a role that would convey such access rights.* –SJ talk 03:02, 3 November 2013 (UTC)

  > Hi SJ, I reworked the paragraph based on your suggestion. Thank you for your help! Mpaulson (WMF) (talk) 19:25, 9 December 2013 (UTC)

Requirements sub-point A

Status: In discussion

Requirements sub-point A [show]

Does anyone agree or disagree with any part of this section?

- This seems to unnecessarily disempower minors, considering how many of our extraordinarily competent, reliable, and talented administrators are smart high school students. If the concern is legal accountability, then a workaround involving a minor's legal guardian should be possible. If the concern is about practical accountability, then a signed statement may be equally effective (and most available remedies would be the same) for trusted community members who are not yet 18. Similar language was intentionally left as "may" instead of "must" in the previous version of the policy, and was not an oversight. –SJ talk 20:33, 24 October 2013 (UTC)
- I'm reposting my response from the discussion below just in case people missed it there: The switch from "may" to "must" was meant to get rid of the ambiguity. My understanding was, in practice, that all community members with access to nonpublic information (except OTRS agents) were required to be 18 years old and the age of majority for their jurisdiction. The reason for this in the current policy, as I understand, was to ensure personal accountability. From a legal standpoint, it is easier to hold an individual personally accountable if they are the age of majority. I saw no reason to leave the ambiguity of "may" in this draft policy if the purpose was to actually have an age minimum. That said, the age minimum (like anything in this policy draft) is not set in stone. It can be raised, lowered, or done away with all together. I'd like to hear what other community members think about the age minimum. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point B

Status: In discussion

Requirements sub-point B [show]

Does anyone agree or disagree with any part of this section?

- This sounds as if the original document of identification has to be passed to the WMF. But this is probably not meant. I understand that the WMF needs some sort of proof of identification but I think it is best to move this to a separate point how this can be done. This section unnecessarily asks for identification documents (or possibly scans thereof) to be handed over to the WMF without considering alternative approaches. As pointed out above this is not just uncomfortable for many functionaries but also in conflict with local legislations. I would like to see here more openness towards solutions that provide the necessary proof of identification but which are more consistent with the preferences and the legal environments of the functionaries. It should be possible, for example, to handle this through the local chapters and possibly third parties. (For example, there exist identification services like Postident in Germany which could be utilized through the WMDE local chapter.) --AFBorchert (talk) 19:34, 22 October 2013 (UTC)
- I agree with AFB: I would strongly approve of any mechanism that does not require community members to send identifying documents to servers in a different country. –SJ talk 20:33, 24 October 2013 (UTC)
- Hi AFBorchert and SJ. This section was indeed meant to require a copy or scan of an identification document to be sent to WMF, not the original document. My apologies for the confusion. That said, we are very open to alternate forms of identification submission and retention and are soliciting suggestions from the community. You may want to see my response in the discussion below. I'd love to hear your ideas. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point C

Status: In discussion

Requirements sub-point C [show]

Does anyone agree or disagree with any part of this section?

- This helps clarify what is being committed to. –SJ talk 20:42, 24 October 2013 (UTC)

Requirements sub-point D part I

Status: In discussion

Requirements sub-point D [show]

Does anyone agree or disagree with any part of this section?

- This requirement has a giant loophole. Why bothering about locked cabinets and password protection when arbitrary third parties with a non-disclosure agreement and unknown policies have unrestricted access to it? Leaks happen. And the best protection against leaks is to minimalize the amount of sensitive materials you collect. Hence, I do not understand why *physical copies of submitted materials* are required. A name and a postal address should be sufficient. (This is at least sufficient in Germany, see de:Ladungsfähige Anschrift.) --AFBorchert (talk) 19:47, 22 October 2013 (UTC)
- A few people have noted that (A) is not clear here. I do not understand the value of keeping other original documents around -- not trusting the initial authority used to verify them and needing to reverify? -- and would appreciate further explanation. There are valid reasons for people, particularly those who live outside of the US, to be wary of having personal documents permanently stored on servers in the US. The reasons for having access to originals that I can think of might be satisfied by either re-requesting them as needed or by having a document-escrow of the person's choice. –SJ talk 20:33, 24 October 2013 (UTC)
- Hi AFBorchert and SJ. As mentioned in the discussion below, we are very open to different forms of submission and retention and would like to hear your suggestions. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point D part II

Status: In discussion

Requirements sub-point D part II [show]

Does anyone agree or disagree with any part of this section?

- In my opinion, this section should be killed. Retention (if any) should only happen during active use of the tools. A three-year period after seems unnecessary. --MZMcBride (talk) 03:07, 21 October 2013 (UTC)
- As pointed out above, it should be sufficient to keep the verified name and postal address of someone with access to nonpublic information. This would also be sufficient in the example you give. There is no need to keep copies of government-issued identifications. --AFBorchert (talk) 19:53, 22 October 2013 (UTC)
- This section seems too broad. An exception should be made for someone whose use of nonpublic information is being investigated (which may be the reason for loss of rights). But otherwise, there should be little need to retain most information. I can see keeping a very-limited historical record to avoid gaming the process: for instance, to keep a single person from identifying many times linked to different on-wiki identities. But some submitted materials (such as copies of formal IDs) could be deleted promptly; others (such as address/contact information) could be deleted soon after rights are given up. –SJ talk 20:33, 24 October 2013 (UTC)
- Thank you for your feedback on the retention period issue, MZ, AFBorchert, and SJ. I'd also like to point out that a related discussion is occurring above in case you want to see what others are saying. I'd also be curious about your thoughts on a 6 month following retirement of access rights retention period mentioned there. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- No opinion yet on the general idea, but I'd note that "If a community member ceases to have access rights, he or she should notify the Stewards" doesn't really make much sense. The Stewards are the ones who revoke access like this in the first place, so why would they need to be notified? — **PinkAmpers&**(*Je vous invite à me parler*) 04:16, 15 November 2013 (UTC)
  - Hello @PinkAmpersand: as an update, that section has now been removed (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&diff=6451564&oldid=6222708) from the policy now. Thanks, 22:32, 3 December 2013 (UTC)

Submitting new materials

Status: In discussion

Submitting new materials [show]

Does anyone agree or disagree with any part of this section?

- Again, this section implies that there is a need to keep copies of submitted materials. --AFBorchert (talk) 19:55, 22 October 2013 (UTC)
- Hi MZ! I wanted to repost what I just said in response to Risker in another portion of this discussion concerning the retention period in case people commenting here miss it up there.

> The reason why we had decided on 3 years is that when discussing potential periods for retention with the Ombudsman Commission, it seemed possible for an investigation concerning the actions of a community member with these kinds of access rights to still be ongoing 2 years after the community member in question had resigned their rights. This could be the case in a particularly complex investigation or one that did not come to the attention of WMF or the Ombudsman Commission until after the community member resigned their rights. That said, I understand that 3 years can be perceived as a long time and if the community believes that investigations of these kinds are all but rarely resolved in a shorter period of time than 3 years, I'm certainly open to hearing what they believe is a more reasonable length of time. Mpaulson (WMF) (talk) 21:40, 22 October 2013 (UTC)
>
> > Probably, if we look to European standards, a reasonable time is ≤\0. --Nemo 08:32, 28 October 2013 (UTC)

Submission methods

Status: In discussion

Submission methods [show]

Does anyone agree or disagree with any part of this section?

- Again, this is unnecessary as there exist alternative approaches to provide a proof of identity. --AFBorchert (talk) 19:58, 22 October 2013 (UTC)

Submission timeline

Status: In discussion

Submission timeline [show]

Does anyone agree or disagree with any part of this section?

- This paragraph fails to outline how the users with access rights will be notified and/or warned. And I think that some time should be given to develop alternative techniques to provide a proof of identity. (This does not need to be covered by this policy. There could be a process that approves alternative approaches.) --AFBorchert (talk) 20:05, 22 October 2013 (UTC)
- As I've mentioned above, we are open to alternative forms of proof of identity. However, I want to assure you that should any requirement submit identification documents or submit identifying information be adopted here, we will do whatever we can to notify any affected users about the new policy and what needs to be done. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Use and disclosure intro paragraph

Status: In discussion

Use and disclosure intro paragraph [show]

Does anyone agree or disagree with any part of this section?

- This section helps clarify what is at stake. –SJ talk 20:42, 24 October 2013 (UTC)

Use and disclosure sub-point A

Status: In discussion

Use and disclosure sub-point A [show]

Does anyone agree or disagree with any part of this section?

- This description does not match the activities of OTRS members. They are not always strictly in the business of preventing, stopping, and minimizing damage to the sites and its users. --AFBorchert (talk) 20:09, 22 October 2013 (UTC)
- Leeway for good judgement would be helpful here and in subpoint B. –SJ talk 20:33, 24 October 2013 (UTC)
- AFBorchert - As mentioned above, the decision as to whether OTRS agents should be included in this policy is still being discussed. However, I would be very interested in your suggestions as to how we could edit this section to include a description of what OTRS does. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- SJ - Could you clarify what you mean by providing leeway for good judgment? Do you have any suggested wording that would illustrate what you mean? Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

> A suggestion for AFB's point: *...solely for activities that protect and help the Sites and their users. Community members with access rights may only use those rights and the subsequent information they access under the policies that govern the tools they used...*
> I'm not sure of the right legal phrasing for good judgement. Perhaps "activities that, in their judgement, protect and help"? I'm not sure how important this is here. But it's usually not clear whether an action actually will have those effects; and the whole point of choosing people for their sensibility is that we are placing that trust in them. So it seems reasonable to me to call that out here. –SJ talk 06:08, 3 November 2013 (UTC)
>
>> Hi SJ, I made some changes based on your suggestion, which hopefully addresses your point. Thank you for the suggestion! Mpaulson (WMF) (talk) 19:37, 9 December 2013 (UTC)

Use and disclosure sub-point B

Status: In discussion

Use and disclosure sub-point B [show]

Does anyone agree or disagree with any part of this section?

- In the current practice of CU cases, some nonpublic information possibly gets public like for example the information which accounts are related. When a CU case includes anonymous accounts identified by their IP addresses, this can be quite revealing. I do not see how this practice is covered by this section. Likewise, it is common practice to publish selected nonpublic information from OTRS correspondence. For example, in a permission case, OTRS members publish the before non-public fact that a copyright owner releases some media or text under a free license. What needs to be exercised is good judgement. Checkusers have a great responsibility when they publish their report of the CU results and likewise OTRS members must carefully judge what can be made public. This section as it stands does not address this. --AFBorchert (talk) 20:22, 22 October 2013 (UTC)
- See above. –SJ talk
- That is an excellent point, AFBorchert. Do you have any suggestions as to how to best address the OTRS scenario that will still protect against the public release of sensitive information often included in OTRS correspondence? As to the CU case, that example was brought up by someone else and

we are trying to figure out a way to address that situation directly in the policy. Any suggestions you have would be greatly appreciated! Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

> Hi AFBorchert. Just wanted to circle back on this and let you know that we added an additional disclosure scenario to this section in the new draft that hopefully addresses this issue. Thank you for your help! Mpaulson (WMF) (talk) 19:43, 9 December 2013 (UTC)

Penultimate paragraph

Status: In discussion

Penultimate paragraph [show]

Does anyone agree or disagree with any part of this section?

- This seems reasonable. --MZMcBride (talk) 03:10, 21 October 2013 (UTC)
- +1 –SJ talk 20:33, 24 October 2013 (UTC)

Final paragraph

Status: In discussion

Final paragraph [show]

Does anyone agree or disagree with any part of this section?

- There are two different e-mail addresses? legal@ and check-disclosure@? This seems confusing. --MZMcBride (talk) 03:09, 21 October 2013 (UTC)
- Actually there's a different situation which should be taken in consideration: if a checkuser living in, for example, Spain, is asked by local authorities to *quickly* disclose and IP of an user posting onwiki its intention to commit suicide. I know this kind of situation has been already managed, but WMF must take into account it re-writing a policy which seems to presume checkusers are criminals by nature. --Vituzzu (talk) 11:54, 21 October 2013 (UTC)
- MZ - legal@ is where anyone who wants to request user information from WMF should send those requests. If a community member receives such a request that falls out of the purview of their role or if they are simply uncomfortable responding to such a request, they should pass those requests onto WMF by sending it to legal@. In contrast, check-disclosure@ is where you should alert WMF that you have disclosed user information to a third party. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- Vituzzu - that scenario should be covered by "In the course of keeping the Sites and its users safe, community members with access rights must sometimes disclose nonpublic information to third parties. Disclosures of nonpublic information may be made to:...law enforcement in cases where there is an immediate and credible threat to life or limb;" Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Notifications

The following discussion is closed: ***closing this since it's been more then a month without response. I think we've reached out to all groups that need it (some a couple times) but if there are others who need it please let me know, I'm happy to try and reach out to others. Will archive in a couple days unless reopened. Jalexander--WMF 20:35, 9 December 2013 (UTC)***

As I already asked on wikimedia-l without answer from WMF: were all the checkusers, OTRS volunteers etc. specifically notified about this draft and discussion which matters them directly, on their email addresses or talk pages? It would be better if the WMF did so, as only WMF knows why we're having this discussion, but time is running: if they don't plan to, can someone use global message delivery to notify them? Objections? --Nemo 06:52, 24 October 2013 (UTC)

> I know all CU/OS/stewards received an email, but I get the feeling that some groups got left out, especially as there is no concrete definition of who is affected by this. --**Rschen7754** 07:00, 24 October 2013 (UTC)
> (e/c)All checkusers, oversighters and stewards were notified by email. I mentioned this above somewhere as well after being asked about it. I know that the enWP ACC tool users (who identify because of their IP access on the tool) were also notified. I have not notified OTRS agents yet because we had not determined exactly how they would be affected, the policy as written did not envision including them (similar to the current policy which puts them into a special category) and the privacy policy was written with that assumption as well (lack of privacy when you email) though I know that it has come up and we would probably need to put an exception into this one similar to the current one. That wasn't added when it was brought up earlier because of the ongoing discussions, my guess at the moment (assuming we continue to check IDs) is that we will have a separate discussion to figure out OTRS which they will obviously have to be notified about. When it came to that I'd probably work with the OTRS admins because I know they have sent mass emails to all agents before. Jalexander--WMF 07:07, 24 October 2013 (UTC)
>
> > Actually I think that all users should be informed about this major change, no matter what user groups they belong to. Of course it is more important for the users who are directly affected by this, but there might be people out there who plan on becoming OTRS agents, checkusers or oversighters on their projects and don't know that this policy may be changed in future. There might be people who want to run for the next steward elections, not knowing about this. Not only users with access to nonpublic information should be informed, but also the people whose nonpublic information we are talking about. I'd like to see some notification about this for all users rather soon. It's not fair to inform only a subset of people instead of all! -**Barras talk** 08:10, 24 October 2013 (UTC)

OTRS users sure weren't - David Gerard (talk) 13:46, 24 October 2013 (UTC)

As Rschen7754 notes, some possibly affected user groups were likely not notified because there's ongoing ambiguity about what the scope of this proposed rewrite is. I believe the current interpretation is that this proposed rewrite would only apply to OTRS administrators, not OTRS users. But at this rate, I think the entire rewrite will be scrapped. --MZMcBride (talk) 14:20, 24 October 2013 (UTC)

@Risker: Would functionaries-en subscribers be required to identify, even though many of them are ex-arbs who no longer hold CU/OS? --**Rschen7754** 18:55, 24 October 2013 (UTC)

If it's about notifications I know I emailed them when we sent out the CU/OS notifications (to make sure they got it). Whether they would need to re identify even if they no longer hold CU/OS to remain on the list is an interesting question I'm not sure had been thought about... Jalexander--WMF 00:09, 25 October 2013 (UTC)

It applies to me and just a couple others (although I guess I might also have to identify for OTRS). It's not like a bunch of folks at the WMF don't already know who I am, so I don't have any problem with identifying again in principle, but it would be a pain... **NW** *(Talk)* 22:29, 25 October 2013 (UTC)

yeah, as usual on these types of edge cases it would have to be a bit of a case by case analysis (since circumstances change etc) but talking with Philippe a superficial look at functionaries-en says that we would likely not force non CU/OS users on the list to identify. Jalexander--WMF 22:41, 25 October 2013 (UTC)

- Note: I'm reaching out to the OTRS admins now to alert all OTRS users of this discussion and the discussion above about if we should include them in the policy. Jalexander--WMF 21:42, 25 October 2013 (UTC)

- Why are not **all** users informed about this discussion? It's good that the people with access to nonpublic information are informed, but I fail to see a reason why the people whose information we are talking about are not informed. I think that everyone should have their say here, and I think everyone deserves it to be informed. Of course the CUs, stewards etc etc are more affected by this, but trying to look at this from outside, as a normal user, I'd like to be informed about that change. There might be users who want to know who deals with their private/nonpublic information and what the rules about this are like. Even thought that is an open discussion and everyone may find this place themselves, I doubt that all users are actively searching for such stuff. Looking at the page, mostly/only people who were informed take part in that discussion. Other people may also have good ideas and wish to comment. I'm really disappointed about the information flow about this. -**Barras** **talk** 12:53, 26 October 2013 (UTC)

The idea was that we were doing this as part of the privacy policy discussion because they are very tightly linked (and changes in here may require changes in the privacy policy). We had a blog post and mailing list announcement (both of which had a whole paragraph talking about this policy) and ran banners both to logged in and anonymous for the privacy policy with links to the blog post in the introduction and links to this policy and discussion on that feedback page. Given that the privacy policy was the center piece of the discussion and we were talking about this in that context it did not seem to make sense to have separate banners for this policy (especially since we were sharing with Wiki Loves Monuments and Fundraising, both of which were pushing for us to lose less space already.. which we were telling them no on). If people think that we should do some more out reach I'm certainly open to it, this is also why we had such a long (and somewhat open ended) feedback period to make sure we could try and get as wide a net of feedback as well. I've always somewhat intended to throw the banners on for another week at one or two different periods over the course of the 4-5 months we are discussing. Jalexander--WMF 10:32, 27 October 2013 (UTC)

Agreed, I work in Account Creation, and I see personal info with every request. Anyone who works with personal information should be notified of this discussion. --Sue Rangell (talk) 19:52, 2 November 2013 (UTC)

feedback from otrs agent

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:51, 9 December 2013 (UTC)***

As for I, I have totally given up with the idea of preservation of confidential data when the US are somehow involved (if the NSA is already involved in recording German president phone conversations or French diplomatic department communications, who are we to hope that our every steps can be private anyway ?).

My trust in WMF ability to provide security to our private information also dramatically dropped with the password leak a couple of months ago.

Hi Anthere. I completely understand your concerns here. The actions of the NSA have shocked and upset us all. As for the hashed password leak, that was a very unfortunate incident and one we are working to ensure never happens again. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)

So what are the risks left ? I see mostly three main ones

disagree with preservation of digital version of id papers

1) that a digital version of my passport get in the hands of scammers. We know some of the risks associated to this, one of which being identity theft. Collection of a bunch of private data (name, email, phone number, postal address...) is one thing. Preservation of official identity paper is another.
I think that's a non-acceptable risk.

We are open to ideas about how the identification documents are stored. Are you against any kind of digital submission or retention of documents or are there certain security measures like encryption that would make this option more palatable to you? If you do not think any digital submission or retention is safe enough, would mailing you identification documents and retaining them in a safe be a sufficient alternative? You may want to look at a related discussion below regarding whether storing identifying information rather than copies of the identification documents themselves would be sufficient and leave some thoughts there as well. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)

Answered below. Anthere (talk)

disagree with disclosure of agent private information to community members not bound to the non public information policy

2) that WMF disclose private information about us (OTRS member for example) volunteers to other volunteers, who may not even be identified in the least (as in "arbitration committee members").

Main risk associated imho would go from mild online bullying to severe irl mishandling. I have very acute memory of this sick person sending me emails threatening my life and the life of my own kids when I was Chair of WMF. I was happy he was in the USA and me in France. I was not happy he knew of my postal address. And I was scared when I met him at the WMF doors irl.

Disclosing private information about us to a lawyer or a policeman is one thing. Disclosing private information about us to an "unknown" wikimedia member not bound by similar rules related to private data is unacceptable.

I'm a little confused about this comment. WMF would not disclose information from the submitted identification documents to other volunteers. Under the applicable clause in this draft, "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." I assume you are referring to the text in the subsection following stating: "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." This section was meant to explain the reasons for retention of your identification information. WMF would not give your identification information to other volunteers in this situation. We would contact you using the information you submitted to us to let you know that ArbCom needs to get ahold of you regarding an ongoing case. Would clarifying that in the policy draft help? (And obviously let me know if I'm misunderstanding your concern here and therefore inadequately addressing it.) Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)

Yes, if this is what you have in mind, I think a clarification of the text would be best. I read that our data may be given to arbcom members for example. Anthere (talk)

ask for mandatorily notification of non public information disclosure about agent from WMF to concerned agent

3) last, that WMF disclose private information about us without having the obligation to inform us it did so.

The draft proposes that *The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors.*

This is vague enough that it may happen that our private data is disclosed to about whoever (who will access our private data thanks to this "permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department" ???), possibly without us knowing.

Consequences may be various (being citing in a legal case without even knowing; having personal information disclosed to spammers or scammers; being sued by an "unhappy customer" after we failed to fix his case on otrs etc.)

A good part of benefit of this agreement would be that covered person better feel accountable.

I think a fitting balance would be that WMF agree to mandatorily inform ANY covered person WHEN and to WHOM his/her information has been disclosed. Accountability both way. Naturally, WMF would also engage itself to inform us when it fucked up (as it did well with the password leak) Anthere (talk)

I agree completely. In fact, the protections that you speak of are currently in the forthcoming "Requests for User Information Procedures and Guidelines". We are working with the EFF to finalize it and will be releasing it publicly soon. The very purpose of these guidelines is to let anyone -- litigants, governments, police authorities -- who wants user information from us know what standards they need to meet before we are willing to release any user information. The guidelines also specify that our default position is to inform the affected user (if we have contact information for them) that such a request has been made and by whom so that the user can use any legal remedies available to them to stop the release of their information. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)

Good (great); Waiting for the forthcoming RUIPG then. Anthere (talk)

Comments

Good points and some scary but true illustrations. I would like to add that I would be a lot more comfortable if I knew that were a scan of my passport to ever be leaked on the internet and I was then subject to identity theft, was then forever internationally blacklisted for credit, falsely thought to be a terrorist by the NSA and could never do business in the USA, or suffered other damages, that the WMF (or their agent with authority to hold the records) had excellent data protection insurance that I could then easily claim something in the order of $2,000,000 compensation to make me feel better about my damage and distress caused by my unpaid volunteer work that happened to require identification. Thanks --Fæ (talk) 14:16, 26 October 2013 (UTC)

Agreed. Anthere (talk)

WMF has secured insurance coverage as deemed appropriate by our Finance department.Mpaulson (WMF) (talk)

Sounds good, as the volunteers that are protected by this insurance, can we look at it please? I would like to know how much I am covered for if someone emailing OTRS tries to take me to court for whatever reason and requires the WMF to reveal my legal identity. Thanks --Fæ (talk) 22:46, 30 October 2013 (UTC)

After Geoff's clarification in a previous section, I now know that there is no "data protection insurance" for volunteers, nor does the WMF have any plans to fix this lack of insurance cover. In this context I feel the answer given that "WMF has secured insurance coverage as deemed appropriate" when the fact is there is no such insurance, was more political spin than a real answer and considering the intention of my comment was extremely clear and illustrated with examples, I feel this was misleading. In practice this means that to get any damages/compensation after suffering identity theft or fraud, a volunteer would probably have to sue the WMF for mishandling their personal data so that in turn the WMF could claim this against insurance that protects them but not the volunteers. I hope that answers to other questions on this page by the WMF have been more straight-forward. --Fæ (talk) 10:43, 15 November 2013 (UTC)

- Thank you for posting these comments here Anthere, I was about to copy them from the mailing list and noticed you already had. Would you mind if I (or you) either adjusted the header or split off #3? I want to make sure that the specific comment on notification gets attention (the other pieces are important as well but I think they are generally covered under other sections which I know are already on the list for discussion and consideration). Jalexander--WMF 06:12, 27 October 2013 (UTC)
  - is that okay this way ? If not clear enough, do not hesitate to edit my part. Anthere (talk)

Illegal

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes (including removal of physical ID) on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:52, 9 December 2013 (UTC)***

In the Netherlands it is illegal to request a copy or scan of a passport or ID card. In the private sector only banks and employers are an exception in that by law.[1] (http://www.telegraaf.nl/binnenland/20791004/__Kopietje_paspoort_verboden__.html)[2] (http://www.cbpweb.nl/downloads_rs/rs_kopie-identiteitsbewijs.pdf) In all other cases it is forbidden to make copies or scans of it. By law we must report any organisation that still requests it, as it is illegal. Romaine (talk) 21:22, 26 October 2013 (UTC)

On the tangential subject of national variations—a slight wrinkle for UK citizens is that we are not required by the state to have any standard ID, and there is no standard identity card even if I wanted one. My passport happens to be the only photo ID I possess, so when that expires next month, I will not have any form of official photo ID to present to anyone. As it happens I have an old form of driving licence, no photo, again UK government does not require me to update to the photo-ID driving licence which was introduced in 1998, so it is just a big piece of paper; it confuses the hell out of people when I try and hire a car. --Fæ (talk) 21:51, 26 October 2013 (UTC)
Hi Romaine, can you clarify the relevancy of the point you make above? Since the WMF is not located in the Netherlands, it's unclear to me. Nathan T 14:28, 27 October 2013 (UTC)

Aren't WMF's esams and knams servers near Amsterdam, The Netherlands? --Krenair (talk • contribs) 14:38, 27 October 2013 (UTC)

Nathan, the actions of the WMF in enforcing policies for Wikimedia volunteers should not just be literally "legal", but being seen as a global charity ought to be lawful. In this case though the WMF may argue the case that it would not be *technically* breaking the law in the Netherlands, the common sense rules for NL businesses and the public still apply. I suggest taking a look at the documents that Romaine has linked to, they seems to support the exact same concerns that have been raised by other volunteers on this talk page. --Fæ (talk) 16:59, 27 October 2013 (UTC)

Romaine, is it also illegal to *provide* such copies? --Nemo 20:13, 27 October 2013 (UTC)

Romaine, how does a business that needs to identify you in the normal course usually do it in NL then? (For instance, if you rent some expensive bit of equipment, the lender would normally need to have some way to keep you accountable).
— Coren (talk) / (en-wiki) 14:04, 28 October 2013 (UTC)

They probably look at the ID card and simply note down the needed data (address, name, date of birth) or put it into their data bank without keeping a scan/copy of the ID card. We've similar laws in Germany. The ID card my be used to verify the data/person, but it is not allowed to retain copies of it. See German laws §§14-20 PAuswG. -**Barras talk** 16:06, 28 October 2013 (UTC)

Just as Barras says, showing the ID card is sufficient (in most cases noting down the info from the card isn't needed). Scanning/copying is only allowed in case of a juridical base: a legal obligation. In other cases it is forbidden to copy/scan. The Dutch government is keen on preventing identity fraud and other forms of fraud with identification. Romaine (talk) 01:35, 29 October 2013 (UTC)

If this is confirmed, it's obvious the policy will have to include at the very least an exception for the Netherlands (and any other country forbidding to make copies of identity documents): the WMF can't solicit, let alone force, anyone to commit illegal activities. --Nemo 06:52, 29 October 2013 (UTC)

Can they do it with people in other countries though? I would've thought that since they have servers in the Netherlands, Dutch law applies to them. --Krenair (talk • contribs) 16:12, 29 October 2013 (UTC)

IMO it would better to establish a standard that works for everyone, rather than have some people with copies of IDs and others with just stored information. Ajraddatz (Talk) 02:07, 30 October 2013 (UTC)

Hi All! Thank you for sharing your concerns here. We are certainly open to ideas on how identification should be handled. Accordingly, I'd like to get some thoughts on a few things below (and please feel respond in-line for the sake of clarity.) Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

First, does anyone have alternate links to the information Romaine provided? I seem to only get error messages when I try them. Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

1. rs_kopie-identiteitsbewijs.pdf on web.archive (http://web.archive.org/web/*/www.cbpweb.nl/downloads_rs/rs_kopie-identiteitsbewijs.pdf)
2. Telegraaf article on web.archive (http://web.archive.org/web/20131101064727/http://www.telegraaf.nl/binnenland/20791004/__Kopietje_paspoort_verboden__.html)

--Fæ (talk) 06:53, 1 November 2013 (UTC)

Second, given the restrictions on providing copies of identification documents to third parties in some countries and the lack of requirements to have any identification documents in other countries, what do you all think would be an acceptable method of checking identification? Would simply submitting your real name and current email address suffice? Should a mailing address or telephone number be required? Are there alternate ways that one can prove their identity other than submission of a government-issued identification document? Should everyone be required to submit their information the same way or should there be different options for people to choose from? If the latter, how do we ensure that the different options are of roughly equivalent credibility? Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

Third, should the information submitted (whether it be a copy of an identification document or simple submission of a name and email address) be verified in some fashion? If so, how? If not, why not? And if so, should it be periodically re-verified and how often? Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

Firstly, a simple method to verify a postal address is to send a letter to it with some token that allows to confirm that it was successfully delivered and received by the intended recipient. This approach is simple and does not break any laws. It just takes some time.
Secondly, I do not see a problem if multiple options are provided where people can freely chose from. You do not need an equivalent amount of credibility, just some minimal threshold which is to be met. No method of identification is safe against falsification. But please remember that you are requiring identification from people who have already trust from the community.
Thirdly, it should be sufficient to simply ask all volunteers who work under this policy to update their address etc. if it changes. --AFBorchert (talk) 19:35, 30 October 2013 (UTC)

And obvious cases should please be handled as obvious cases. Some prefer pseudonyms but many of us work already with their real name all the time (like me). You will find my full name on all my major wiki user pages, you find a backlink to Wikimedia Commons at my private website (http://www.andreas-borchert.de/), whose domain is owned by me (there are public records with my name and address at DENIC), and whose IP address (currently 217.10.8.60) when submitted to RIPE delivers multiple contact records including AFB13-RIPE (https://apps.db.ripe.net/search/query.html?searchtext=AFB13-RIPE&searchSubmit=search) which delivers my full address including phone number. You need of course a general solution for the identification problem. But I would appreciate it if obvious cases (like mine) need no further bureaucratic procedures. --AFBorchert (talk) 19:49, 30 October 2013 (UTC)

Thank you for your thoughts and suggestions, AFBorchert.

Postcards to verify address have been mentioned multiple times. Another option, to verify at least name and potentially more, is a symbolic payment: PayPal uses it, it's the only legal identification method for bank accounts "portability" in Italy, etc. A 0,01 € bank transfer to your SEPA bank account will be an extremely easy and cheap option for many in EU (you could also pay it back, I hope WMF doesn't pay fees for such SEPA payments). It wouldn't work for everyone, of course; just adding to the list of ideas. --Nemo 20:09, 31 October 2013 (UTC)

I would like to add into the mix that any trusted user that is, or has been in the past, a trustee or director of a legally incorporated Wikimedia Chapter or Thematic Organization has public records of their directorship available as a public record. I believe that in most countries this means that there is a record of their directorship that is fairly easy to link to on the internet. Directorships have been verified against legal IDs (which acts as protection against money laundering) and have been accepted by the WMF under the Chapters Agreement. Personally, I don't mind sending the WMF a link to my online directorship records as they are already a public record; this avoids the bizarre discussion we will have when the WMF asks me for valid photo ID and I say I don't have any, as it is not required in the UK. --Fæ (talk) 07:04, 1 November 2013 (UTC)

I work in Account creation, and I see personal info in almost every request. As an identified editor, I had no problem with the scanned ID, and will happily do it again. A symbolic paypal payment is also acceptable. I don't think a postcard would work for me. I live in a remote area and sometimes I get mail 2-3 months late. (although I have no problem with that as long as that is taken into account) I am worried a bit that there will soon be an admin requirement for this. I don't want to be an admin, but more and more I am finding that it is necessary to become an admin just so that I can do the things I do on Wikipedia. --Sue Rangell (talk) 19:42, 2 November 2013 (UTC)

I agree with most comments made there

- most businesses requiring ID information record first name, last name, dob, country-region-date for issuing the ID document, and unique number of the document. They do not keep a copy of the ID but usually ask to "see" the ID paper and record data themselves in front of you. Ideally, it would be a declaration of honour you would require from us. Alternatively, we sent (in some encrypted fashion if possible) the scan, you record the data and you delete the scan.
- I recently moved; wrote my US bank to record the new postal address; they wrote to my former address for confirmation and ask me to send back a document. Very simple way to check addresses. Easy to do the same with the email address for confirmation. May be renewed once a year if suitable (as in… once a year, WMF send a new year eve wish card to all its agents and agents have to answer "thank you" :))
- Token payment is an option as well
- and yes, please rely on cases where people are or have been board members or staff within chapters (or on WMF board for that matter ;)). All those people already disclosed mandatorily their ID data to their chapters.
- use opportunities of face to face meetings to do an irl ID check-up (wikimania, wikimedia events when WMF staff is there) rather than electronic one.

Anthere (talk) 10:24, 7 November 2013 (UTC)

Statement from user:aschmidt

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:52, 9 December 2013 (UTC)***

One of the most fundamental priciples in data-protection law is that no data shall be collected and saved unless it is absolutely necessary to do so. There is no point in collecting scans of OTRS sysops' and maybe even agents' official documents. If the WMF is interested in learning who works in OTRS it would suffice to store their names and adresses only. This is why it would be disproportionate to keep any scans. For the same reason there is no legal justification for keeping all this data for years after a Wikipedian has ceased to contribute to OTRS.

To put it clearly: The Wikimedia Foundation is a big U.S. foundation worth millions of Dollars that runs hundreds of huge websites in some 200 languages. Those volunteering in the OTRS team provide online support for free that the Foundation would otherwise have to pay for by hiring agents. When I contribute for free as a volunteer to OTRS I expect the WMF to except us from any liability whatsoever as long as we are acting in good faith. Also, I think it is not only a matter of whether only OTRS sysops or agents, too, should be subject to this new policy. If it would be enacted I would quit German-language OTRS even as an ordinary agent.--Aschmidt (talk) 19:30, 28 October 2013 (UTC)

Hi Aschmidt! Thank you for your sharing your feedback. I'd like to hear more about what concerned you about this draft. We are trying to change this draft such that it gets to a point that most people are comfortable with its requirements. We certainly are not trying to drive you away from being an OTRS agent!

First, do you believe that WMF should keep any kind of identification policy at all, as discussed above? If we do continue to have an identification policy, you mentioned that you think real names and addresses would suffice. Did you mean email address or physical addresses? What way would you feel comfortable submitting that information? Do you think that information should be verified in a particular way?

You have also indicated that you believe retention of such information for 3 years following the retirement of access rights is too long. What would be a more appropriate retention period in your eyes? There has been a more detailed discussion about this particular topic above that might interest you.

And finally, if we do retain an identification policy of some kind, do you believe that OTRS agents should be subject to it (assuming that the policy adequately addresses your other concerns)? Why or why not?

Thanks again for taking the time to help us make this policy draft better. Mpaulson (WMF) (talk) 18:35, 30 October 2013 (UTC)

Stuff to think about

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:53, 9 December 2013 (UTC)***

Just to make clear, I do not wish to reidentify if this policy becomes live. I identified when people could still go to a local WMF office and then make themselves clear for a local WM office member, and so identify themselves. I send my ID two years ago and then it was destroyed and only a few basic stuff were needed (name, date of birth, nationality etc). I cannot believe that rewriting an exisiting policy which works fine for over six years is more important than improving existing tools and developing new tools for the hardworking community. You even make it harder for the volunteers to do their work. Also I'm not comfortable with the WMF keeping my ID somewhere in the USA, or even with some basic information. You know who I am. That should be enough. You should spend time at the tools we actually need (finalizing SUL, global rename, global checkuser, global blocking etc) instead of writing new fancy tools such as wikilove, the thank button and visual editor. I know it's important to attract new volunteers, but please do your best to keep the existing ones as well. FYI, I'm one of the most active stewards and meta CUs and the active CU on commons. It's your loss if I quit, not mine. I have enough useful things to do. And I know more people think about this the same as I do. Some might say: "well, those are the consequences if you change a policy. Approximately 10% quits." But I disagree with that. You should listen to the people who do the work. And do something with their feedback. I'm also waiting for three months almost for an answer of Philippe (unrelated to this). That illustrates how the staff works here with the volunteers I guess. It's easy to answer easy questions, but less easy to answer to more difficult questions apparantly. Thanks for your time. (And don't get me wrong, I am happy with some things, though not with everything...) Regards, Trijnsteltalk 12:24, 3 November 2013 (UTC)

> Hi Trijnstel - Thanks for your comments, which definitely resonate with me. We actually take the feedback from volunteers in these consultations quite seriously - and modify or propose ideas accordingly. I agree that, if we require improved identification, we probably should explore avoiding a new identification with the same information. In response to the feedback, one proposal - which we make above - is to eliminate all identification requirements, and that would address some of your concerns, I believe, and in fact render the job of volunteers a bit less administrative. I'm sorry about the lack of response for one inquiry. If you resend your question to me, I will try to get someone to handle it for you. I completely agree that your quitting is our lose ... so please don't. :) Our volunteers are so critical to the movement and its mission. Without any exaggeration, you are the inspiration for all of us. Geoffbrigham (talk) 00:41, 6 November 2013 (UTC)
>
>> Hi Geoff. Thanks for answering. Here a follow-up as I don't really get what you mean. You say:
>>
>> - *"if we require improved identification, we probably should explore avoiding a new identification with the same information"* - so that would mean that the re-identification rule would still apply in the new policy (with the 3 year retention in it), but what do you mean with "new identification with the same information"? Saving name, age etc? (which I'm not fond of either)
>> - *"one proposal - which we make above - is to eliminate all identification requirements"* - so everyone can identify then? Even if you're not yet 18 or 21 (depends in which country you live)? That's a really bad idea imho. And it doesn't address my concerns at all, which is that the Wikimedia Foundation will keep the ID of the volunteers who just want to help. With the posibility to sue them if they do something wrong, instead of making the WMF responsible. Or maybe I didn't understand you correctly?
>>
>>> Sorry, I was not that clear after thinking about your question some more. I agree with you in principle that we need to minimize the burden of identification and reidentification on our volunteers. So I'm open to an easier re-identification procedure where we retain the basic information (name, date of birth, point of contact). With known volunteers, we could figure out simple ways to get that information to hopefully decrease the administrative burden. I do think that, if we require identification, we would need to record the name, date of birth, and contact information to be consistent with the intent of the applicable Board resolution. We do not need to keep the identification, but we do need to record the identifying information to be honest by the Board resolution.
>>> If we eliminated the identification process at WMF, we would simply rely on the community processes to properly vet volunteers per the age requirements and capabilities; that way WMF would be retaining no personal information on our volunteers. (After reading the full consultation, that is an approach I'm beginning to consider seriously, though we would need the WMF Board to agree.)
>>> As to responsibility of the users, we could put limits on the liability, which I discuss a bit more here. To be clear, it is a hard case to imagine where we would ever sue a legitimate volunteer who is acting in good faith. My concern is about someone who, in bad faith, for example sells nonpublic information for personal gain. That is the "test" case that I'm trying to figure out. As I say, I discuss this a little more here. Thanks for the great questions and expressing your legitimate concerns, which I take quite seriously. Geoffbrigham (talk) 23:47, 6 November 2013 (UTC)
>>>
>>>> But then would local communities be responsible for handling private information? On English Wikipedia, ArbCom does vet volunteers, but I would feel uncomfortable with them having my personal info. On Commons/Wikidata/Meta etc. it's just a vote by the community. --**Rschen7754** 09:07, 7 November 2013 (UTC)
>>>>
>>>>> Under the proposed approach, I think it would be up to each community to decide what the acceptable standard would be and whether identification would be required. The number of questions that have arisen with respect to WMF holding the information and frankly the arguable ease by which one might be able to submit a fraudulent ID suggest to me that we should seriously consider eliminating all WMF identification. We would need to be clear in the privacy policy that WMF cannot identify those who have access to nonpublic information but

that communities are free to set their own standards, including identification processes. We could set minimum standards, such as requiring those with access to keep the information confidential (even if they are not identified). It is not a robust approach, but, if I am reading the discussion fairly, most in this community consultation seem to be rejecting a strong verification, accountability system that is manageable in a practical way, which is fine as long as we are honest about it in the privacy policy. Geoffbrigham (talk) 19:45, 22 November 2013 (UTC)

Btw, no need to look at my question, Maggie said a few days ago that she would take care of it. Trijnsteltalk 16:33, 6 November 2013 (UTC)

Thanks, let me know if you need anything there. Geoffbrigham (talk) 23:47, 6 November 2013 (UTC)

WMF board, FDC, etc.

The following discussion is closed: ***Closing given how long it has been since the last edits will archive in a couple days unless reopened Jalexander--WMF 20:54, 9 December 2013 (UTC)***

I assume that candidates for the WMF board, FDC, etc. would have to identify regardless of what is decided here - is that correct? --**Rschen7754** 09:28, 6 November 2013 (UTC)

Correct. Geoffbrigham (talk) 20:06, 22 November 2013 (UTC)

That would be my understanding under the inescapable international requirement to meet money laundering regulations. Both trustees on the WMF board (once elected) and FDC members have influence over the disposition and management of significant funds. I would support some form of independent but legally meaningful identification (it does not have to be through the WMF) for anyone in any Wikimedia organization taking a direct part in how significant funds are spent.
Saying this, I think there is room for less onerous requirements for "insignificant" funds, such as being on a judging panel for prizes but not in control of the budget allocated, where the total being given away is less than $1,000. In those circumstances the fact that Wikimedia *should* always default to open processes, means that if someone starts giving their mates prizes in an arbitrary way, or the competition was not properly promoted so only someone's pals even take part, then at some point there will be public complaints; knowing this, anyone that fiddles the system for small amounts of money would be pretty daft and find themselves having to pay the money back. I have put "should" in italics here as I have recently found myself arguing the case for openness within Wikimedia organizations in situations I never expected and sadly find myself becoming more jaded over time with the ability of our community to implement this theoretical ideal. --Fæ (talk) 16:41, 6 November 2013 (UTC)

Pedantic lawyerly point about use of "age of majority"

The following discussion is closed: ***Closing given how long it has been since the last edits and large changes in draft since then. Will archive in a couple days unless reopened Jalexander--WMF 20:55, 9 December 2013 (UTC)***

The current policy refers to the user being "over the age at which they are capable to act without the consent of their parent in the jurisdiction in which they reside." The proposed policy instead refers to the user being "at least the age of legal majority under the laws of the jurisdiction in which they reside." I would suggest that the existing wording (or other similar wording) is preferable because it corresponds more precisely with the expressed purpose of the age requirement, viz. ensuring that users with access to sensitive information have "legal accountability" for their actions. Let me illustrate by reference to New Zealand law. The age of majority in New Zealand is technically 20 (Age of Majority Act 1970, s 4(1)).[3] (http://www.legislation.govt.nz/act/public/1970/0137/latest/DLM396495.html) However, 18 and 19 year-olds are fully legally accountable for their actions and their parents have no legal authority over them. Contracts can be enforced against them (see the definition of "minor" in the Minors' Contracts Act 1969, s 2(1)).[4] (http://www.legislation.govt.nz/act/public/1969/0041/latest/DLM392356.html) So the proposed policy would seem to exclude 18 and 19 year-olds in New Zealand, despite this being completely unnecessary in terms of the rationale.

Interesting point. If someone is 18 or 19 in New Zealand, can they enter into a binding contract by themselves without a parental cosignatory? Geoffbrigham (talk) 22:08, 15 November 2013 (UTC)

Yes, since the Minors' Contracts Act doesn't apply to them. I recall that when I went to university aged 17 I had to have a parent sign the contracts, but when I turned 18 I was able to sign them without a parental cosignatory. Neljack (talk) 12:37, 18 November 2013 (UTC)

I apologise for raising such a technical point, but it is what we lawyers are here for, isn't it? :) Neljack (talk) 11:30, 10 November 2013 (UTC)

Oh and while I'm at it I suppose I may as well raise a couple of other unclear points that have just occurred to me. Firstly, would the copy of the ID need to be notarised (by a lawyer, Justice of the Peace, etc)? Secondly, I don't have a government photo ID. What would happen in such cases? Neljack (talk) 11:51, 10 November 2013 (UTC)

Hi Neljack! The age of majority language has been removed from the current draft. Hopefully, that resolves this issue. Mpaulson (WMF) (talk) 23:11, 3 December 2013 (UTC)

The proposed policy would not need a notarized document, though it would require a government photo ID. We are thinking about proposing another version of this policy, and I guess we could think about adding an alternative identification procedure. What would you suggest? We have also suggested that maybe we simply ditch this policy. What do you think about that? Geoffbrigham (talk) 22:08, 15 November 2013 (UTC)

There is no government photo ID in the UK as has already been highlighted above along with some alternative suggestions for process. I think by now that a clear majority of unpaid volunteers participating here are concerned or alarmed about the WMF holding onto their ID. Perhaps you would like to see a !vote if that is ambiguous? --Fæ (talk) 03:54, 16 November 2013 (UTC)

I think it would be perfectly reasonable for the Foundation to retain the information provided the documents aren't kept, though I have no objection to ditching the policy if that is considered appropriate. As for alternative forms of disclosure, I suppose if somebody required me to prove my identity I would send them a copy of my birth certificate, possibly accompanied by a statutory declaration (witnessed by a Justice of the Peace or lawyer) affirming (on pain of criminal penalties) that it is my certificate. Neljack (talk) 13:09, 18 November 2013 (UTC)

Hi Neljack. The ID requirement has been removed from the current draft of the policy. Thank you for taking the time to share your thoughts on the draft! Mpaulson (WMF) (talk) 23:11, 3 December 2013 (UTC)

Community Committees

The following discussion is closed: ***Closing per comment from Michelle at end. Will archive in a couple days unless reopened. Jalexander--WMF 18:38, 11 December 2013 (UTC)***

Hi, as an OTRS administrator, I would be affected by the policy proposal since it stipulates several changes to the identification procedure. As an affected user, I would like to emphasize a point others have already raised (embedded in wider critiques), which, to me, is by far the most disturbing aspect of the policy proposal. According to the proposed text of the access to nonpublic information policy (henceforth "Policy"), "[s]ometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining [...]" I would like to express my strong opposition to this. As I cannot conceive of any legal reason that would require a disclosure to a "community committee," I am puzzled as to why the Wikimedia Foundation would consider that a necessary or, for that matter, acceptable use of my data.

First, it does not fit into the overall approach of the Policy. At least members of the Election Committee and OTRS administrators do not in their respective roles participate in community processes on individual Wikimedia Wikis. It is therefore not plausible that identifying information about members of either group is passed to community committees for undoubtedly they have no competence to investigate issues that arise within the affected users' capacity as members of these groups in first place. The passing of identifying information about members of these groups to community committees can never serve to fulfill the explicit intent of the identification process ("This helps to increase accountability and ensure against misuse of information entrusted to community members with access to nonpublic information."): Whenever identifying information about such member is provided to a community committee, that must necessarily be related to a member's action unrelated to their treatment of nonpublic information; this cannot be in the spirit of the Policy.

Second, the term/phrase "community committee" is not defined in the Policy and, as far as I am aware, not elsewhere. As of now, the German-language Wikipedia's adaption of the English Wikipedia's Arbitration Committee (the *Schiedsgericht)* does not require members to be identified to the Foundation, and the scope of the two committees' activities differs considerably. Furthermore, there are ad-hoc committees for certain tasks, such as evaluating contests or organizing local elections. In light of this, it is not possible for me to understand, based on the Policy, which "committees" qualify as "community committees" within the meaning of the Policy.

Third, it is not possible at a reasonable effort for members of affected user groups to assess the risk of an undesired use of identifying data by community committees. The Wikimedia Foundation is committed to certain goals and ideals and also has a history of being transparent about internal staff policies. When a member of an affected user group releases identifying information to the Foundation, they can place some trust in the Foundation to process/store/use the information in a responsible manner. They can also keep track of the development of the Foundation and decide if they still desire to provide the Foundation with the identifying information. However, it is entirely impossible to keep track of changes to the composition or policies of community committees in hundreds of Wikimedia Wikis. If a community committee on the Italian-language Wikipedia requests identifying information about me from the Foundation and the Foundation provides the information (be it justified or not), the identifying information gets into the hands of users unknown to me and potentially unknown to the Foundation, residing somewhere in the world. This is unacceptable. Under the current phrasing, providing the Foundation with identifying information is tantamount to providing it with the competence to provide it to third parties effectively free to use the information for purposes other than those envisaged in this Policy. — Pajz (talk) 16:48, 16 October 2013 (UTC)

1. +1 There is a long history of issues with emails sent with an expectation of remaining private or confidential later being released or leaked without permission one way or another when managed by community controlled lists and archives. This does not inspire confidence for how identifying private records would be respected under this policy and the systems being proposed. --Fæ (talk) 16:10, 18 October 2013 (UTC)
2. strong +1 as well. Why would personal information about an OTRS member be disclosed to community members often anonymous. That escapes me. Anthere (talk)

Hi Pajz, Fae, and Anthere! I fear there has been a miscommunication. WMF would not disclose information from the submitted identification documents to other volunteers. Under the applicable clause in this draft, "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." The text in the subsection following stating: "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." is not meant to say that we would disclose the identifying information about you to other community members. This section was meant to explain the reasons for retention of your identification information. WMF would not give your identification information to other community members in this situation. We would contact you using the information you submitted to us to let you know that ArbCom needs to get ahold of you regarding an ongoing case. Would clarifying that in the policy draft help? We could also get rid of that portion talking about community committees and ArbCom all together if it's too confusing. What do you think? Mpaulson (WMF) (talk) 18:55, 31 October 2013 (UTC)

Perhaps adding another sentence like "In that scenario, the WMF would notify you through the information you provided to us about this, but your contact information would not be given to the community members"? --**Rschen7754** 19:05, 31 October 2013 (UTC)

Yes, you do need to clarify the wording. My English comprehension has been tested as excellent, even for a native speaker, so reading this again tells me that under section D, the WMF is free to share any information it wishes with any (unnamed) third party to protect its property or rights. In legal parlance, the unqualified terms "property" and "rights" are so wide as to accommodate virtually anything, including weird stuff of potential rather than defined value like reputation of the Wikimedia projects or the WMF "brand", disputed domain name registrations, or disputed claims of copyright of its materials or future "community logos". To emphasise the point, "third parties" means *anyone*. --Fæ (talk) 19:25, 31 October 2013 (UTC)

Dear Michelle, thank you for your detailed response. I would certainly appreciate a clarification in the draft, though I am indifferent as to whether that should take the form of a removal of the passage about community committees alltogether or a rephrasing in the spirit of Rschen7754's proposal above; as for me, I cannot conceive of a reason why a community committee would need to reach identified users through these means. If a user is ready to answer questions from community committees, they won't have a problem reaching him; if he does not leave contact information and does not react to posts on his talk page, odds are that he just doesn't wish to be involved in Wikipedia or Wikimedia matters anymore. And while these committees play a vital role in our community, they are not ultimately conducting legally relevant investigations, so why bother identified volunteers? But as I said, I don't really care about that as long as the Foundation doesn't pass the information to members of these committees.
Which brings me to another passage you quote, and which Fae criticizes above. I concur with Fae's point. I'm not happy with (D) in its current form. As Fae points out, the provision is lacking any specification of the third party involved. I am sure you have given this more thought than I have, but couldn't this at least be narrowed down to law enforcement agencies? In another comment of yours, you suggest to change the wording from "(D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors" to "(D) needed to protect the safety of others or WMF staff, contractors, systems or property" and give the example of an identified community member breaking into your building. Earlier today, you provided another example of a volunteer who "purposefully planted any viruses, malware, worms, Trojan horses, or malicious code that could harm our technical infrastructure in violation of the Terms of Use or that could expose the personal, nonpublic information of other users." In both cases I assume that the party you would share the information with is a police agency and/or a state attorney (I presume this varies among different legal systems). This suggests to me that you could narrow down the third party recipients of the information as proposed. I do have some other criticism with respect to the points (A)–(D), but I do think that a specification of "third party" would be a grave improvement anyway. I would be interested in your thoughts on this. Regards, — Pajz (talk) 23:01, 31 October 2013 (UTC)

Hi Pajz. I understand your concern regarding the term "third party" in relation to subsection (D)(i). We are currently reevaluating that section in light of community feedback and will be responding accordingly in a thread below. Because the community committees topic has been resolved, we are going to close this thread and continue the discussion about which scenarios sharing submitted materials would be appropriate in the other thread. Thank you for your feedback and patience! Mpaulson (WMF) (talk) 00:17, 10 December 2013 (UTC)

Retrieved from "https://meta.wikimedia.org/w/index.php?title=Talk:Access_to_nonpublic_information_policy/Archives/2013&oldid=16362352"

This page was last edited on 26 February 2017, at 17:57.