Tor Fundraiser Donor Privacy Policy
Drafted by Sue

Backstory: Originally I put this draft on a Mozilla etherpad which later became uneditable when Mozilla I gather deprecated support for them. Therefore, I have moved it here, so people can edit & comment. Over the past month, on the etherpad, it's gotten lots of input, especially from Nick, & lots of revisions have been made. I am about 90% sure the information below is accurate, and I would very much appreciate people pointing out where/if I'm wrong.

Status: I have shipped the draft to Nick & asked him if he will ask the board to discuss & vote on it. Please therefore don't change the text of the draft any further: please just comment instead.

This donor privacy policy has been approved by the Tor Project board of directors.

The Tor Project respects donor privacy and welcomes anonymous donations. If being anonymous is important to you, the best way to preserve your anonymity is by donating using a method that doesn't disclose your personal information.

If you provide personal information as part of the donation process, it may be collected and retained by third-party service providers and/or the Tor Project, as described below. The Tor Project has very little influence over how third-party service providers, such as PayPal, may collect and use your information. We recommend you familiarize yourself with their policies, especially if you have privacy concerns.

When you donate to the Tor Project, depending what mechanism you use, we may learn your name, the amount you donated, your email address, phone number and/or mailing address, as well as any other information you provide. We may also learn incidental data such as the date and time of your donation. The Tor Project will never have access to your financial data, such as your credit card information.

We aim to be careful with your information. If you have provided your email address, we will email you once to thank you and give you a receipt. If you opt in during the donation process, we may email you again in future. If you donate more than $5,000 and we know your name and address, we are required to disclose it to the IRS in Schedule B of the Form 990. But, that information is redacted from the publicly-available version of our Form 990. We will never publicly identify you as a donor without your permission.

We do not publish, sell, trade, or rent any information about you. For our records, we retain your name, the amount of your donation, the date of the donation, and your contact information. Access to that information is restricted inside the Tor Project to people who need it to do their work, for example by thanking you or mailing you a t-shirt.

The Tor Project very much appreciates all its donors. Thank you for supporting Tor.

((Stuff below is deleted text or is comments. Some is still relevant, some is probably not.))

Stuff to be verified:
-- I am assuming the Tor Project has no access to financial information such as CC numbers through any donation mechanism.
-- I am assuming Tor can access user info such as browser/OS for some donation methods, but I might be wrong.
-- I am assuming that the Tor Project knows it can redact donor information from Schedule B, and that it does redact it.
-- I am assuming that access to donor information inside Tor is actually restricted to people who need it for their work -- e.g., Roger for thanking, Juris for t-shirt mailing, finance people for reporting, etc.
-- I am assuming there's no data retention policy or practice, either committing to retain or committing to destroy.

We may use anonymized donor information for our promotional and fundraising activities.* We may publish any comments donors provide to us and use them in our promotional materials.** We will never publicly identify a donor by name, unless they have given permission.***[The version of this sentence that made it into the text above is better as it is stronger and given that these three sentences are making it into the donor policy as well having the "we-dont-publicly-identify-you" just once should be enough. gk]

* [we ought IMO to be about 9000% more specific about that. What ***exactly*** do we mean by anonymized there? We can't be vague about it, since we're supposed to be the experts in the field of what it means to anonymize stuff. For example, we could say 'We may use anonymized donor information (for example, a mean of some datum in a group of 100 donors)..."]

** [well hang on, really? even if they self-identify? Even if the comment is "Hello my name is Alice Smith and I live at 123 main street in Oppressionberg, Repressionstan, and I like what you've been doing! Hooray for the tor project! Down with the Repressionstani regime!"?]

*** [Define 'publicly'. I presume telling the bavarian illuminati and the lizard people wouldn't count. But some folks are worried not only about being identified publically, but also to the secret masters of bonk-oif.]

When do we delete donor data that we learned, if ever? Who internally will use/access that data, do we have anything in place that prevents this from being leaked? << This is a great question and I will ask have just sent an email to Tor's finance people asking. If they don't know, I will follow up later with Roger/Nick :)

More questions: what mechanisms do we use to ensure that donor data remains private? Is it, "if we get rooted, I hope you used an anonymity tool" or do we encrypt? Under what legal pressure would we divulge? Do donors get better or worse privacy than non-donors who contact us? (either possibility will smell bad, even if it's the best we can do.)