FEDERAL ELECTION COMMISSION
Washington, DC 20463

MEMORANDUM

TO: **The Commission**

FROM: **Commission Secretary's Office**

DATE: **April 22, 2014**

SUBJECT: **Comments on Draft AO 2014-02 (Make Your Laws PAC, Inc.)**

Attached is a late submitted comment received from Sai. This matter is on the April 23, 2014 Open Meeting Agenda.

Attachment

MYL PAC
% Nick Staddon, Secretary
122 Pinecrest Rd.
Durham, NC 27705

Federal Election Commission
Office of General Counsel
999 E Street, N.W.
Washington, DC 20463

MYL PAC Comments re other comments on AO 2014-02

April 22, 2014

Dear Commissioners:

Please accept the following late comments on behalf of Make Your Laws PAC, Inc. (MYL PAC) in response to other parties' comments to date on AO 2014-02.

1. Louis Joyce

Joyce is not correct that "[a]ll Bitcoin donations are inherently anonymous". Bitcoin transactions are *pseudonymous*, *partially* traceable, and identified to the extent that the Bitcoin user *chooses* to identify themselves. However, Joyce is correct (as discussed in our comments) that Bitcoin transactions are not as auditable as KYC account transactions, and that it is not (currently) feasible to be *certain* that a given address belongs to a given person.

This is why we proposed the $100 limit — by analogy to *identified* contributions of cash. Our proposal mandates that a contributor provide 2 USC 431(13) identification (*before* getting a linked address for contributions). As with attestations, that *always* relies in part on trust.

A targeted Bitcoin address collision is not merely "mathematically unlikely"; it's *statistically impossible* without a cryptographic attack sophisticated enough to completely break Bitcoin. However, it is certainly possible for Bitcoins (just like cash or prepaid credit cards) to be stolen, or for access to Bitcoin addresses to be shared (just as checking accounts can be). Part of the standard attestations we will require (as specified in our AOR) is that the contribution comes from the contributor's own funds (or funds shared with a spouse but made in the contributor's own name), that they are not a foreign national, etc.

It is certainly possible to programmatically collect a large number of identities and make ≤$100

Bitcoin contributions claiming to be from each. This would be clearly illegal for the erstwhile contributor (under the FECA, plus multiple felonies under other titles). Within Bitcoin itself, there would be no easy way to detect this if the Bitcoin is properly laundered.

However, contributions *aren't* just within Bitcoin. With *all* payments (not just Bitcoin contributions), we will frank the IP address used when connecting to our website (where the identification information, attestations, etc need to be made), and we already use a custom server module[1] to detect connections made over Tor. Users detected as coming from Tor will not permitted to make financial contributions, and many purportedly different contributors coming from the same IP address would raise a flag for hold pending manual review.[2]

While Joyce is correct (as we discussed at length in our comments on AO 2013-15) that refunds cannot (currently) be reliably made *within* Bitcoin, we specified that in no event would we do so. We will *only* issue refunds in US currency, to *identified* contributors. Someone with adequate technical skill could circumvent our donation process by analyzing the block chain to determine our (non-disclosed) Bitcoin holding address, but we would easily identify such transactions, and dispose of them as proposed in Draft B for non-identified contributions.

Finally, we intend to itemize *all* of our Bitcoin contributions and expenditures (regardless of amount), and would welcome an advisory opinion that *mandates* such itemization.

Sincerely,
Sai
President & Treasurer
Make Your Laws PAC, Inc. (MYL PAC)

sai@makeyourlaws.org
https://makeyourlaws.org/fec/bitcoin

---

[1] https://github.com/MakeYourLaws/rack-tor-tag + https://www.torproject.org/projects/tordnsel.html.en. Feel free to visit https://makeyourlaws.org using the Tor browser bundle (https://www.torproject.org); our site prominently shows the green Tor onion if you do so, signalling our detection of such connections.

[2] It is certainly possible for multiple distinct, legitimate contributors to have the same IP address (e.g. due to NAT and dynamic IP addresses), so this is more of an art than an exact science. Likewise, many US citizens live overseas and/or use legitimate VPN connections, so geolocating an IP address to a foreign country is also not a definitive reason to believe that a contribution is unlawful.

We are required to make "best efforts" — not to be perfect, nor to conduct forensic traffic analysis. Our proposal meets this standard. If anything, this issue applies even more to e.g. credit cards than to Bitcoin (under our proposal), since those have no $100 limit and can be purchased semi-anonymously with cash.