web.archive.org

Inside the Effort to Crowdfund NSA-Proof Email and Chat Services

Written by DJ Pangburn Contributor

14-17 minutes

Back in 1999, Seattle-based activists formed the communication collective Riseup.net. The site's email and chat services, among other tools, soon offered dissidents a means of encrypted communication essential to their work. Fourteen years later, Riseup is still going strong. In fact, they've been fighting the US state surveillance apparatus longer than most people have been aware of the NSA's

shenanigans. Now, the collective is hoping to expand, given the gross privacy transgressions of the NSA and US government as a whole.

"What surveillance really is, at its root, is a highly effective form of social control," reads an August Riseup newsletter. "The knowledge of always being watched changes our behavior and stifles dissent. The inability to associate secretly means there is no longer any possibility for free association. The inability to whisper means there is no longer any speech that is truly free of coercion, real or implied. Most profoundly, pervasive surveillance threatens to eliminate the most vital element of both democracy and social movements: the mental space for people to form dissenting and unpopular views."

The impetus behind the project

is Riseup's struggle to keep up with new user demand for an email service that doesn't log IP addresses, sell data to third parties, or hand data over to the NSA. Riseup will also be able to expand its considerable anonymous emailing lists, which features nearly 6 million subscribers spread across 14,000 lists. Their Virtual Private Network (VPN), which allows users to securely connect to the internet as a whole, will also be made more robust. What Riseup can't do is offer its users an anonymous browsing experience, but that's not their aim.

To offer Riseup to more users, Free Press's Joshua Levy, Elizabeth Stark (an open internet advocate who has taught at Stanford and Yale), as well as others at the StopWatching.Us campaign (backed by Mozilla) recently launched an Indiegogo crowd-funding effort on

behalf of the group. They hope to raise $10,000 in order to provide Riseup —which is run by volunteers—with a new server, hardware, and software capabilities. In short, they want to expand their reach so that internet users have another alternative to email services such as Gmail, Yahoo, and Hotmail.

To get a clearer picture of what StopWatching.Us and Riseup are doing, I spoke with Levy, Stark, and an anonymous Riseup collective member. We talked about how the crowdfunding money will be spent; how Riseup helps users avoid NSA, as well as state and local repression; and why, contrary to reports, the Tor Browser bundle is still the best option for anonymous, encrypted browsing. (As of today, the crowdfunding campaign reached it's $10,000 goal, but the organizers are

hoping to exceed that total by a good margin.)

Tell me a bit about your respective work with and use of Riseup.net as StopWatching.Us organizers.

Josh Levy: The StopWatching.Us coalition launched in the days after the first Snowden leaks in early June. As we put together our plans and our communications infrastructure, we agreed that we didn't want to rely on services like Google Groups—which apparently had been compromised—to host our sensitive communications. We naturally turned to Riseup, which has been providing services to activists for more than a decade and is run by dedicated volunteers, many of whom are friends.

It turned out that we weren't the only ones turning to Riseup: thousands of other individuals, spooked by stories

about NSA spying on peoples' Gmail and Hotmail accounts, turned to Riseup too. The result was that Riseup's servers could get overloaded with all of the new activity, and they didn't have the hardware or manpower to keep up. Hence the idea to launch a campaign in support of them.

> "***Activists who use Riseup aren't really contending with the NSA as their threat model. Typically, their problems are the local police, or other forms of state repression.***"

Elizabeth Stark: We really wanted to go with an email provider that was independent and not part of one of the major centralized tech companies. Riseup was the obvious choice, with their commitment to privacy, supporting activists, and fighting surveillance. The community felt much more secure not

having it in the hands of a big tech company that would be more vulnerable to surveillance, but we were having some issues with the lists. Specifically, some of our messages were arriving significantly late, and when we inquired with Riseup about this, it had turned out they were slammed with new users and some very large lists using their fairly limited servers.

The answer, it seemed, was to get some new and faster servers to be able to handle all of the traffic. Josh and I rallied several friends within the StopWatching.Us group to pitch in and launched the campaign in conjunction with a contact at Riseup.

About how many activists and other internet users currently use Riseup's encrypted email?

Anonymous Riseup member: This question depends a bit on what service

we are talking about, and how we measure use. If it is just email, we have about 68,000 email accounts right now. We don't have the ability to measure how many people are actually using those, but we clean out unused ones every three months, so it is reasonably accurate. If we are talking about mailing lists (which the StopWatching.Us campaign is focused on), we are are the largest non-profit mailing list service on the internet, with the exception of universities. We've got 5.4 million subscribers to all the lists we host. We do other things as well, such as hosting servers for groups, chat, VPN, etherpad, as well as documentation, education and free software development.

We just learned about NSA's incredible ability to decrypt anonymous encryption services.

Tor is far more vulnerable than previously imagined. Is Riseup seriously able to contend with the NSA?

Josh: These revelations have shown that the NSA is attempting to crack into nearly every effort we make to keep our communications private. And yet, some interceptions are harder that others. Using services like Riseup raises the cost of the NSA's spying infrastructure. If an activist is using Riseup's servers —which aren't part of the PRISM program like Gmail or Yahoo! mail—and that activist is also using a common encryption system like GPG, it becomes much harder for the NSA to view the contents of her messages. The more we raise the costs of the NSA's spying, the harder its job will be. That said, no one will really be safe until we reform the laws that have given the NSA cover to

practice its mass surveillance in the first place.

Elizabeth: First of all, the Tor issue isn't one of Tor's vulnerability as a service, but instead how a vulnerability in Firefox was used to compromise people using Tor that were accessing a specific server—one that the Feds had compromised. So the lesson to be learned here is: 1) no technology is completely foolproof where there are a lot of areas for compromise (browser, servers, etc.), and 2) be careful about what servers you're accessing if you're looking for complete anonymity.

I'd actually like to remind any readers of this quote from a recent New York Times piece on the NSA foiling encryption: "Because strong encryption can be so effective, classified NSA documents make clear, the agency's success depends on

working with Internet companies—by getting their voluntary collaboration, forcing their cooperation with court orders or surreptitiously stealing their encryption keys or altering their software or hardware."

> "***We built the internet, and some of us have helped to subvert it. Now, those of us who love liberty have to fix it.***"

We definitely don't have risks 1 and 2 happening with Riseup, which are arguably two of the biggest risks. That said, I don't speak for Riseup, but it's also highly unlikely that there's an undercover agent working with them in the way that it's been reported they have at large tech behemoths.

Riseup: Activists who use Riseup aren't really contending with the NSA as their threat model. Typically, their

problems are the local police, or other forms of state repression. Riseup believes it is critical that essential communication infrastructure for the movement be controlled by movement organizations and not corporations or the government.

We cannot rely on corporate providers for confidentiality of sensitive communications. Not only are their commercial interests at odds with what we are doing, but monitoring and association mapping gives them (and by extension the state) the ability to build a detailed map of how our social movements are organized. This gives them precise information about what links should be disrupted in order to disrupt larger social movements.

Nevertheless, how does Riseup plant to contend with the NSA? We have

been working on this for some time and it is a multi-faceted approach: we support people and projects who are working through the legal system or applying political pressure. We have been employing state-of-the-art encryption technologies for transport and storage of our user's information. Unfortunately, those technologies are not quite there yet. That is why we have been working on a plan for some time. Over the last year we've been working on a project to roll out a series of radically new services based on 100% open source and open protocols. They will be easy to use and will protect our user's data from everyone (including us).

How does Riseup avoid handing over data to the NSA?

Riseup: This one is both simple and complicated. Riseup doesn't keep IP

logs of our users, so we aren't acting as deputized agents of the state, collecting information on our users that we have to turn over if we get a legal request to do so. Although this is the default configuration for servers, we are not required by US law to collect this information, and so we do not. However, how do we avoid handing over data to the NSA? This one is more or less speculation, because we don't know what data the NSA is getting through its passive full-pipe monitoring efforts. Although surveillance is nothing new (governments have always targeted activists with surveillance and disruption, especially successful activists), what we are learning day to day is on a very different level.

Those who imagine a government can be trusted to police itself, when given

the ominous power of precise insight into the inner workings of everyday life, are betting the future on the ability of a secretive government to show proper self-restraint in the use of their ever-expanding power. If history has shown us anything, it is that the powerful will always use their full power unless they are forced to stop. At Riseup, we have felt for the last few years that the window of opportunity to counter the rise of universal surveillance is slowly shrinking. Now is our chance to establish a new reality where mass numbers of people are using encryption on a daily basis.

Elizabeth: Now, of course it's possible that the NSA is decrypting traffic by tapping into the pipes, but given the strength of a lot of encryption and the unlikelihood they'd have a back door

into Riseup, it's fairly unlikely that they've managed to decrypt this traffic.

After this round of fundraising, do you imagine another will be launched to add even more servers, hardware, software development, etc.?

Josh: It's always possible that we or another group will launch another round of fundraising to help support Riseup. That said, if we meet our goal of $10,000, it'll go a long way toward helping Riseup continue to be a pillar of the activist community.

Riseup: And we will engage in our regularly annual fundraiser closer towards the end of the year.

> ***"Those who imagine a government can be trusted to police itself, when given the ominous power of precise insight into the***

> ***inner workings of everyday life, are betting the future on the ability of a secretive government to show proper self-restraint in the use of their ever-expanding power.***"

Is Riseup considering an anonymous browser at some point in the future?

Riseup: We believe that the best anonymous browser that exists out there right now is the Tor Browser Bundle, and we recommend that to our users. We do not believe that our efforts are best spent in that area, as the Tor Project is doing a wonderful job with that browser. Combined with the TAILS project, which Riseup supports, there is nothing better.

What other efforts are currently happening in the anti-surveillance

activist world?

Elizabeth: We're gearing up for a whole host of new legislative efforts designed to counteract surveillance in one way or another, and our role is in building grassroots support for these bills. For example, we as a coalition were recently able to garner 15-20k phone calls within 24 hours in support of the Amash Amendment, the amendment from MI Rep. Justin Amash to defund the Section 215 surveillance capabilities of the NSA, including the domestic phone metadata collection. The effort narrowly failed by 7 votes, but it was widely considered to be a victory considering the amount of support it did receive. Amash has said he's busy working on a new approach, and various other folks in congress are working on bills of their own.

If we as a coalition can get that many

calls within such a short period of time (and with virtually no advance notice), there's a lot more we can do with more time and preparation. We're also planning a big day of action in DC around the 10th anniversary of the Patriot Act on Oct 26 against surveillance. More details to come soon.

Any final thoughts on anti-surveillance activism and Riseup?

Elizabeth: Having providers like Riseup is critical to enable people to engage in free speech and to communicate in a more secure manner. One of the scariest things we've seen recently is how the government has compelled services such as Lavabit to comply (and compromise their users' security) or shut down. And even in the wake of shutting down, the Lavabit founder is facing potential legal action

because he shut down. We need groups like Riseup to stand up against this kind of bullying on the part of the government, especially when it involves the very people that are fighting for transparency and against unconstitutional surveillance.

As Bruce Schneier recently said, "We built the internet, and some of us have helped to subvert it. Now, those of us who love liberty have to fix it."