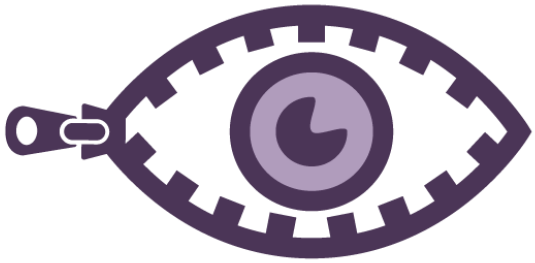


Open Privacy

Research Society

2018 End of Year Report

11th February 2018 —10th February 2019

Introduction

Open Privacy was founded on the belief that the world can be better. We started as a group of researchers and technologists who were frustrated by the ever growing stranglehold of surveillance capitalism and the harm it was causing marginalized and at-risk communities. We wanted to build an organization that served those that mainstream groups ignore: sex workers, queer people, those impacted by intimate parter or family abuse, and human rights activists, to name just a few.

On the 11th February 2018 we officially incorporated the Open Privacy Research Society as a non profit society in B.C.

The response we received from the community was overwhelming, within hours our inbox was filled with emails ranging from congratulations to offers of donations, volunteer support and interest in joining our board.

Over our first year we put in place the infrastructure necessary to sustain our unique research society. We have built relationships within and across communities. We conducted innovative research in the field of metadata resistant communications and made significant headway in understanding how to deploy such technology in the real world.

As we move through our second year as a society I want to thank all of our supporters, institutional donors, volunteers and staff. Without you Open Privacy and the vital work we do, could not (and would not) exist.

Our mission has only just begun, and I invite you to join us again as we continue to gain momentum and help build a better world.

Sarah Jamie Lewis

Executive Director, Open Privacy Research Society

OPEN PRIVACY
RESEARCH SOCIETY

Projects

Cwtch

Communications metadata is known to be exploited by various adversaries to undermine the security of systems, to track victims and to conduct large scale social network analysis to feed mass surveillance. Metadata resistant tools are in their infancy and research into the construction and user experience of such tools is lacking.

Cwtch began as an extension of the metadata resistant protocol Ricochet to support asynchronous, multi-peer group communications through the use of discardable, untrusted, anonymous infrastructure.

Cwtch aims to solve many of the problems faced by the marginalized communities that we serve but primarily it solves the **anonymous-first-contact problem**.

Many people in the communities we serve wish to build relationships with others in the community or people outside of their community, but they wish to preserve their privacy and minimize the risk of someone discovering information about them that they do not wish to share publicly.

Cwtch is designed to allow communities to build safe & secure spaces that can provide discussion platforms, advertisement services, shared lists.

At the end of our 2018 year we delivered the first alpha version of Cwtch. This has been met with great excitement and enthusiasm from the wider community, attracting a number of volunteers who have contributed code, bug reports, testing, translations and documentation.

This project is directly funded by donations to Open Privacy.

OPSec

Late in 2018 we were awarded a microgrant from the Digital Justice Lab to kickstart a project called OPSec.

While the grant was modest, we were able to sponsor an Open Privacy staff member to volunteer their time at an advocacy organization that serves outdoor sex workers.

Through that volunteering we were able to identify multiple security and privacy issues that directly impacted those who were supported by the organization.

As an example, our staff member found that public internet access terminals were not configured to delete browsing history or saved data, this led to the personal and private information of many members being accessible - including saved passwords for email and tax return credentials.

Our staff member first worked to mitigate the potential and future harm by cleaning up the computers, and adjusting the settings to delete browsing history and cookies, and is now working with the organization to ensure that public internet access remains accessible and preserves the privacy of those who use it.

This experience has been invaluable in informing our research directions and we will continue to seek and engage opportunities that allow us to work closely with community groups.

This project was initially funded by a grant from Digital Justice Lab, we continue to seek donations and funding to extend this pilot project.

Shatter Secrets (Unfunded)

Shatter Secrets uses strong cryptography to distribute “shares” of a decryption key to people on the other side of an international border so as to technically prevent their compelled disclosure. Existing approaches are subject to subtle weaknesses in their protocol, such as allowing border agents to intercept secrets during transmission, or employ social engineering against remote confidantes.

Our approach uses threshold cryptography so that some minimum number of designated secret keepers must meet physically in person at the destination before the protected information can be recovered, with special care taken in its design to prevent common compulsion techniques and social engineering vectors.

In May 2018 we began the process of partnering with journalists and activists in western Asia, South America, and southern Africa, with a focus on user research to explore their needs, workflows, and use cases, as well as subsequent evaluation of our tool, to transform the research prototype into a fully fledged solution.

Unfortunately, after progressing to the final rounds of a major grant application process, this project was not selected as one of the grant recipients.

Shatter Secrets remains a project that we believe is important and we will continue submitting grant applications and seeking additional partnerships with media organizations and activists as opportunities arise.

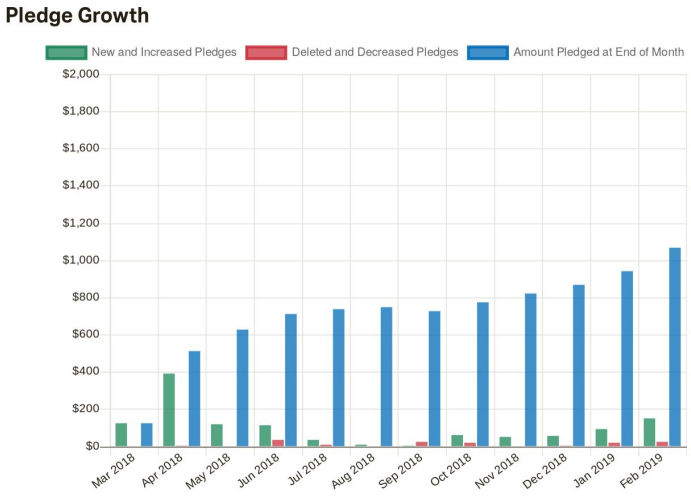
Donations & Support

In our 2018 financial year[1] Open Privacy heavily relied on support from individual donors, rather than organizational or governmental grants. The flexibility of this funding has allowed us to produce research that would be impossible to produce in other environments.

Patreon

At the end of the 2018 financial year, Open Privacy had 88 pledges contributing **$942 USD/month** via Patreon. We saw an initial spike in support when we launched our Patreon in March 2018, and have seen consistent pledge growth throughout the 2018 year.

In the 2018 year supporters on Patreon contributed 15.7% of all donations.



Patreon Pledge growth during the 2018 Financial Year

[1] February 11th 2018 to February 10th 2019

PayPal

Open Privacy received **$6437.63 CAD** via Paypal donations.

CryptoCurrencies

In the 2018 year Open Privacy received donations in the following cryptocurrencies:

- Bitcoin – **3.90 BTC**
- Monero – **10.23 XMR**
- Zcash - **3.89 ZEC**

Cryptocurrency donations made up 61.27% of all donations to Open Privacy in the 2018 year.

Grants

In the 2018 year Open Privacy applied for several grants. We received funds from the following organizational donors:

- Digital Justice Lab - **$3000 CAD**

Benefit Events

In the 2018 year Open Privacy was the beneficiary of one externally-organized event:

- Blockchain Against Evil - *$1368.39 CAD*[2]

[2] The event took place in the 2018 financial year, however the donation was booked in our 2019 financial year.

Travel Assistance / Event Discounts

In the 2018 year members of Open Privacy have accepted travel assistance and/or discounts to attend conferences and events from the following organizations:

- Privacy International - Gender & Privacy Workshop
- Citizen Lab - Canadian Cybersecurity Dialogue
- Reboot Communications - Privacy and Security Conference
- Access Now - RightsCon Toronto

Organizational Structure

The Open Privacy board approved 3 staff positions, and hired 3 full time staff members in the 2018 financial year:

- Dan Ballard – Director of Engineering (Hired August 2018)
- Sarah Jamie Lewis – Executive Director (Hired September 2018)
- Erinn Atwater – Research Director (Hired October 2018)

All three hires are Open Privacy founders. All three staff members also sit on the Open Privacy board (but did not participate in votes to approve their contracts or staff positions).

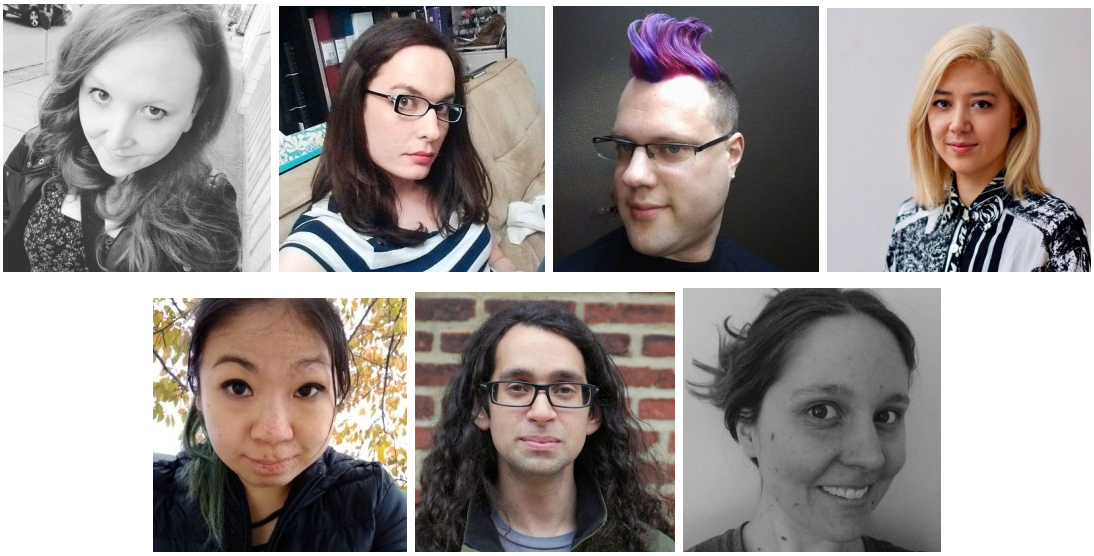
Reflecting our role and mission as a research organization, our largest expense in the 2018 financial year (accounting for 85% of all expenses) was that of staff salaries (**$32,386 CAD**). All Open Privacy staff members are paid the B.C. minimum wage - we note that this is not a living wage and well under the market rate for the technical and organizational skills that they provide.

It is the goal of the executive committee and the board to provide suitable & sustainable compensation for all Open Privacy staff members.

The Open Privacy Board of Directors

In addition to the 3 founding members of the board, 4 new board members joined Open Privacy during the 2018 financial year. As per the bylaws, no board members are directly compensated for their work as directors of the board. Three of the board members are staff members of Open Privacy.

- Sarah Jamie Lewis - Chair (Executive Director)
- Erinn Atwater - Vice Chair (Research Director)
- Dan Ballard - Treasurer / Secretary (Director of Engineering)
- Yuan Stevens - Director
- Cynthia Khoo - Director
- Norman Shamas - Director
- Cecylia Bocovich - Advising Director



Financial Statements

On March 19th 2019 the board voted to give the Executive Committee authority to commission a Notice to Reader engagement in line with the estimate of $2000 as provided by Smythe CPA.

A copy of the Notice to Reader is provided with this report.

This does not constitute a formal audit of the Open Privacy Research Society. The board did consider estimates for a formal audit, but the cost would have exceeded 10% of our income and the board ultimately determined this would not have been a good use of funds.

It is the goal of the Executive Committee and the board to engage in a formal audit once our funding levels are sufficient to support it.

Land Acknowledgement

The Open Privacy Research Society would like to acknowledge that the land on which we work is the unceded territory of the Coast Salish Peoples, including the territories of the xʷməθkwəy̓əm (Musqueam), Skwxwú7mesh (Squamish), and Səl̓ílwətaʔ/Selilwitulh (Tsleil-Waututh) People.