

HELPING ACTIVISTS
STAY SECURE ONLINE:

Reflections from RightsCon 2023



Sections

[Summary](#)

[PART 1:](#)

[Workshop summary](#)

[Ideas](#)

[Insights](#)

[PART 2:](#)

[Identifying key solutions](#)


[Taking action](#)

[Lead a challenge](#)

Summary

In June 2023, [ExpressVPN](#) hosted a workshop at RightsCon focused on advancing human rights through digital means. This event brought together human rights defenders from across the world to share their ideas on how technology can aid their efforts. The workshop began by identifying challenges faced by various participants, followed by brainstorming tailored solutions.

The workshop was facilitated by Lauren Hendry Parsons, Privacy Advocate at ExpressVPN. Fellow panelists included Francesca Bosco, Chief Strategy and Partnerships Officer of cybersecurity and digital rights NGO [CyberPeace Institute](#); Rhona Tarrant, Head of Editorial at social news and strategic intelligence agency [Storyful](#); and Shirin Mori, Senior Design & Research Lead of the NGO [Electronic Frontier Foundation \(EFF\)](#).



Part 1

Workshop summary

Ensuring digital safety for activists is a global challenge

The workshop attracted participants from various regions, including Switzerland, the Netherlands, the United States, and Uganda, among others. The attendee list included human rights defenders (HRDs), activists, lawyers, technologists, journalists, and educators. This diverse representation highlighted the universal nature of challenges faced by activists and underscored the potential for global and locally adapted solutions.

Activists need digital access, safety, and security

The workshop's central focus was on the importance of digital access, along with digital safety and security. Key points included:

- The detrimental impact of prolonged internet shutdowns on HRDs, especially those in exile, and the urgent need for consistent internet access.
- The necessity for trust-building in the digital sphere, especially for civic partners who depend on digital tools daily.
- The importance of open-source, free, and affordable solutions to protect networks and enable collective action.
- A strong demand for tools to counter surveillance, interrogation, and imprisonment, and implement rapid response strategies, including techniques for erasing digital footprints.

- The need for secure methods to capture, collect, and distribute evidence—especially regarding hate crimes and state violence—underscoring the need for robust documentation and storage tools.



"I accompany and support HRDs in exile. I want to see the problem of long-term internet shutdowns fixed so HRDs have consistent internet access."

"I am a human rights lawyer, and I care about (the) collection of evidence of hate crimes and police violence in Brazil."

"I'm a human rights defender. We have been under attack, and I'm looking for specific tools regarding surveillance, interrogation, imprisonment, and rapid response."

- WORKSHOP ATTENDEES

The role of technology in serving community needs—collaboration and accountability

- The workshop raised important concerns about the growing influence of big tech corporations and their potential roles in government-led repression of rights.
- Discussions about the challenge that tech monopolies pose to digital rights.
- Many HRDs stressed the urgent need for education on digital surveillance, particularly focusing on common vulnerabilities like smartphones.
- There was a strong call for the development and adoption of user-friendly, peer-to-peer, or open-source alternatives. These tools aim to empower individuals, reducing their reliance on major tech corporations.
- Attendees strongly advocated for legislative measures against spyware and other forms of surveillance technology. They also emphasized the need for civil society campaigns to drive change in this area.



"I'm a fact-checking journalist. I'm constantly trying to keep my team up-to-date with digital security practices, digital and physical investigations, and reporting."

"I want to create legislation against spyware. I conduct pressure campaigns to bring about change."

"I design Corporate Social Responsibility (CSR) strengthening programs on how to protect networks and galvanize collective action in closed civic spaces. I want to understand what open-source, free, and affordable solutions should be supported."

- WORKSHOP ATTENDEES

Three universal priorities

Three key universal priorities emerged throughout the workshop:

- 1. A need for universal access to encrypted communication tools to protect sensitive information.**
- 2. A need for universal digital literacy and skills training to enhance awareness of digital threats and protective measures.**
- 3. A need to share information, resources, and tools, to align efforts and maximize impact.**

Actions and next steps? Read on

The below outlines the proposed actions and next steps to address the challenges identified during the workshop.

Ideas for solutions

Some solutions to assist activists and HRDs, as discussed during the workshop, include:

TECH SOLUTIONS

- Easy-to-use encryption technology with self-destruct features to safeguard data in case of a breach.
- Secure communication methods, like affordable or free VPNs or other encryption protocols.
- Open-source operating systems for devices, to counteract the surveillance risks associated with preloaded spyware in many mobile operating systems.
- Low-tech or no-tech communication alternatives, including methods for secure physical message transfers and unconventional internet routing.

SOCIAL SOLUTIONS

- Educational programs highlighting technological vulnerabilities and promoting the use of open-source software as a countermeasure.
- Workshops to train participants in verifying the authenticity of apps and software, ensuring they are not compromised.
- A digital trust badge system for easy identification of verified secure tech tools and platforms.
- Alert apps that notify a network of allies if someone is arrested or in danger, promoting the creation of effective communication networks.
- Guides offering step-by-step procedures for evidence collection and access preservation during arrests.

Insights from the workshop discussions

Some solutions to assist activists and HRDs, as discussed during the workshop, include:

Recognition of urgency

Many problems facing activists and others are happening right now and require urgent solutions.

Holistic approach

It's not just about handing activists the right tools; we also need to focus on training people and effecting change through policymakers.

User-centric design

Digital tools, important for online safety, need to be well-designed and easily accessible.

Advocacy and awareness

Activists need better education on how they can be spied upon and how to avoid this unwanted attention.

Collaboration as a driving force

The best way to spread tools and training is through collaboration: HRDs of different backgrounds need to connect and stay in touch.

Financial support and resource allocation

NGOs and similar organizations need sufficient funds to hire their own cybersecurity experts to develop the necessary tools.

Empowerment through decentralized technologies

Considering that much of today's surveillance is conducted by the same companies that innovate, the focus should be on creating more decentralized and open-source technologies.

Cybersecurity processes and governance

HRDs require clearly defined cybersecurity policies and governance to safely adopt new technologies in their defense work.

Part 2

Turning talk into action

The big picture: Identifying key solutions

Ten clear themes emerged around the types of solutions needed:

- 1 **Develop comprehensive training programs.**
- 2 **Foster collaboration and partnerships.**
- 3 **Promote user-friendly tools.**
- 4 **Increase funding opportunities.**
- 5 **Advocate for policy changes**
- 6 **Foster decentralized technologies.**
- 7 **Raise awareness and provide resources.**
- 8 **Support local partnerships**
- 9 **Establish emergency response networks.**
- 10 **Prioritize collaborative research and development.**

Who needs to be part of the solution?

While a wide range of experts participated in the workshop, a broad spectrum of collaborators and partners is needed to make these ideas a reality, including:

- **Technology and cybersecurity experts** from academic institutions and research organizations.
- **Media organizations** specializing in investigative journalism and digital security reporting.
- **Online platforms and social media companies** committed to user privacy and safety.
- **International human rights bodies and organizations**, such as the United Nations and Amnesty International.
- **Local and regional government entities** responsible for protecting human rights and promoting digital security.
- **Grassroots organizations and community-based initiatives** focusing on digital rights and security.
- **Ethical hackers and cybersecurity professionals** for vulnerability assessments and testing.
- **Internet service providers (ISPs) and telecommunications companies** interested in promoting secure and private communication.

Taking action

As we transition from discussion to action, this segment outlines concrete steps and initiatives we plan to undertake, building on the insights and discussions from the workshop. Our aim is to transform the solutions discussed into practical, real-world applications that can significantly benefit the activist community.

Sharing a digital security resource library

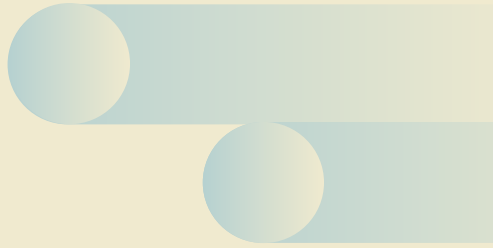
A resource library offering comprehensive and practical guidance on improving digital privacy and security. This was completed at the start of 2024 and can be found on the [ExpressVPN Rights Center](#).

Starting a cohort/community

Our goal is to establish a quarterly virtual meet-up to facilitate discussions, skill-sharing, and problem-solving around the key themes outlined above. This group will include participants from the workshop who have committed to continuing their collaboration as a cohort.

The framework for these calls needs to be decided. For example, in the initial call, cohort volunteers could present their work, a problem they are facing, or a specific project they need help with, with the goal of receiving feedback and help from the group. These calls may also include a discussion section focusing on key themes.

Ultimately, we would like these cohort calls to focus on collaboratively working towards a specific project, which will be decided upon based on the outcomes of the initial calls.



Want to get involved or lead a challenge?

It's time to consider how each of us can contribute to the transformative ideas we've explored. Whether you see yourself as a leader of change or as a crucial contributor, your involvement is key to turning these concepts into reality. Here are the steps for those ready to take on the challenge:

1. Decide if you want to be a solution lead or a contributor

- a. Nominate yourself accordingly in the Collaborative Project Map
- b. [Collaborative Project Map \(for all workshop attendees to add to\)](#)

2. If you want to be a solution project lead:

- a. Build your team and your roadmap.
- b. Reach out to the collaborators identified earlier, including workshop participants and additional stakeholders, to form your project team.
- c. Establish clear communication channels and collaboration frameworks.

3. Co-create solutions

- a. Analyze the issue and chosen solution, and develop an action plan that identifies the most critical and achievable goals within a two-year timeframe.
- b. Rescope the project if necessary to focus efforts and resources more effectively.

4. Develop a solution roadmap:

- a. Create a detailed roadmap outlining specific milestones, tasks, and timelines for your
- b. Break down larger goals into manageable steps and assign responsibilities to collaborators.

5. Execute pilot programs:

- a. Launch pilot programs in select regions or communities to test and refine solutions.

6. Report back on impact

- a. Share the results of your projects with workshop participants.



Contact us

If you would like to speak with any of the contributors to this report, please reach out to safe@expressvpn.com