Security, Privacy and Grassroots Environmentalism in the Philippines

Mikaela Brough, PhD Candidate

Royal Holloway, University of London
Supervised by: Professor Rikke Bjerg Jensen, Professor Martin Albrecht

Agenda

1. **Design and Activism**
2. **Why Grassroots Environmentalism in the Philippines?**
3. **Methods**
4. **Findings**
5. **So what does this suggest?**

What does it mean to design for activists?

- A key motivation behind existing literature on information security and activism is the desire to **design for activists**.
- This body of work often involves conducting interviews with activists in different contexts to **identify design needs**. These interviews are usually remote, but sometimes take place in person. [2, 5].

What does it mean to design for activists?

- A key motivation behind existing literature on information security and activism is the desire to **design for activists**.
- This body of work often involves conducting interviews with activists in different contexts to **identify design needs**. These interviews are usually remote, but sometimes take place in person. [2, 5].

The particularity of activist settings makes a ground-up approach essential. Accordingly, I:

- Use an **ethnographic approach**.
- Conduct immersive fieldwork in activist groups.
- Conduct ethnographic interviews and participant observation to surface the *undercurrents* [6] of information security practices – **less visible realities within social movements that influence decision-making**.

Why Grassroots Environmentalism in the Philippines?

Definition of Red-Tagging

Acts of labelling, branding, naming, and accusing individuals and organizations as being left-leaning, subversive, communist, or terrorist, used as state agents and non-state actors against those perceived to be 'threats' or 'enemies of the State'. – Supreme Court Justice Marvic Leonen in Zarate v. Aquino III

- Known for being **one of the 'highest-risk' environmental movements in the world** [1].
- Repression here refers to *"widespread red-tagging, surveillance, and harassment"* [4, p. 1] and associated violence.
- Law enforcement agencies are also known to use advanced forms of **targeted electronic surveillance** against social movements of concern [3].

Fieldwork

- **Timeline:** Fieldwork took place in July and August of 2024 and from February to June 2025 in Cebu City (project area established nearly 2 years ago).
- **Local partner groups:**
  - PRIMARY: small enviro legal activism group
  - SECONDARY: larger human rights activist group
- **Political context:** ICC arrest of former president Rodrigo Duterte, General Election 2025

Personal photo from April 2025, taken with permission.

Methods

- **Participant Observation:** Protests, public hearings, large community events, group meetings, security trainings, workshops, other trainings, election events, and church services.
- **Interviews:** Ethnographic interviews – some repeated, some paired.
- **Other:** 4 security trainings workshops, documents, visual methods.
- **Reflexive thematic analysis:** Iterative analysis conducted in stages, informed the design of tailored interview guides.

Personal photo from March 2025, taken with permission.

Mobility

Participants explained that their movement networks were highly geographically dispersed and interconnected. The security priorities of these activists were strongly shaped by the **constant need for mobility**, which often took them through contentious areas.

> *"It was a funny experience that a guy once said 'how do you know I'm in the bar', well because you're wearing the tracker!"*
>
> – P27

> *"...So nothing's actually a confidential document. It's very risky, especially in the provinces."*
>
> – P19

Mobility

Participants explained that their movement networks were highly geographically dispersed and interconnected. The security priorities of these activists were strongly shaped by the **constant need for mobility**, which often took them through contentious areas.

"It was a funny experience that a guy once said 'how do you know I'm in the bar', well because you're wearing the tracker!"

– P27

"...So nothing's actually a confidential document. It's very risky, especially in the provinces."

– P19

"It's just the information is so difficult to actually access, and this is because of fears of the security."

– P24

Key undercurrent

Participants perceptions of their own risk were framed by how they interpret the security risks and desires of **other groups and areas** across regions.

Authority

- Groups generally used hierarchical organisational structures *within groups* but formed large non-hierarchical networks *between groups*.
- Groups also engaged in skill sharing and security trainings.
- Despite this, the question of who gets to make decisions about security was fraught, with **different kinds of expertise in conflict**.

Authority

- Groups generally used hierarchical organisational structures *within groups* but formed large non-hierarchical networks *between groups*.
- Groups also engaged in skill sharing and security trainings.
- Despite this, the question of who gets to make decisions about security was fraught, with **different kinds of expertise in conflict**.

Example

At an activist gathering, a participant said their group was trained by a digital rights organisation and sometimes trains rural communities. They noted a persistent problem "matching what people want" to technical advice. P32 added that during a recent visit to Palawan, they found many rural groups in their network already had security experts.

Key undercurrent

Security norms are both driven by *top-down* tech expertise as well as *bottom-up* lived expertise of violence.

Resources

Despite holding certain views about information security practices, some ideal practices could not always function easily due to differences in resources. Ideas surrounding resources were not only about people's own resources, but also those of others in their network.

Resources

Despite holding certain views about information security practices, some ideal practices could not always function easily due to differences in resources. Ideas surrounding resources were not only about people's own resources, but also those of others in their network.

Example

P7 recounted how communities don't have "WhatsApp or they don't have Viber or Telegram, the easiest way they could get internet connection is through Messenger." They explained that for other organisers that say they *only* use Telegram (as a security practice), the community appoints one person with the most data to download Telegram as a point person.

Key undercurrent

Technology choices were **sometimes driven by pervasive but differential conditions of low data**.

Cultural Codes

- Participants described how they flexibly adapted their behaviour based on **how they believed their actions to be culturally perceived**.
- For example, participants noted that they would make a **conscious effort to fit with the prevailing technological norms of particular identity markers**.

Example

P3 showed me that in Signal he only a few contacts, claiming that Signal is associated with Manila. P3 explained that in that in his small group, *"no one really has that time for all that"*. One time they were doing a training from a UK group who would only communicate on Signal and P3 helped his group *"in downloading yeah.. they're like* **what even is this?**"

So what does this suggest?

- By paying attention to what people do and say in their everyday lives (**first-order practices**), this work suggests practices are shaped less by the features of technologies themselves and more by the social and cultural contexts in which they emerge.
- To understand information security decision-making in social movements, it is important to be immersed. This means **rethinking the kinds of prevailing study designs** used in security research that *only* prioritise **second-order knowledge** (how people justify and codify their first-order practices).

So what does this suggest?

- By paying attention to what people do and say in their everyday lives (**first-order practices**), this work suggests practices are shaped less by the features of technologies themselves and more by the social and cultural contexts in which they emerge.
- To understand information security decision-making in social movements, it is important to be immersed. This means **rethinking the kinds of prevailing study designs** used in security research that *only* prioritise **second-order knowledge** (how people justify and codify their first-order practices).

Overall

This means that programmes that aim to design for activists **are incomplete** without empirical information about first-order practices.

Photo by Wayne Grazio, CC BY-NC 2.0

I would like to thank the participants who generously gave their time and trust.

And I would like to thank you for listening!

mikaela.brough.2022@live.rhul.ac.uk // mikaelabrough.github.io

References


Carlos H. Conde.
Philippines Worst in Asia for Killings of Environmental Defenders.
Human Rights Watch, 2024.


Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas.
Defensive Technology Use by Political Activists During the Sudanese Revolution.
In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 372–390. IEEE, 2021.


Steven Feldstein.
The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance.
Oxford University Press, 2021.


Council for People's Development and Governance and National Union of People's Lawyers.
Civil Society Report on the Misuse and Abuse of Combating the Financing of Terrorism Measures in the Philippines.
Technical report, 2025.


Harry Halpin, Ksenia Ermoshina, and Francesca Musiani.
Co-ordinating Developers and High-Risk Users of Privacy-Enhanced Secure Messaging Protocols.
In *Security Standardisation Research: 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings 4*, pages 56–75. Springer, 2018.


Yong Ming Kow, Yubo Kou, Bryan Semaan, and Waikuen Cheng.
Mediating the Undercurrents: Using Social Media to Sustain a Social Movement.
In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 3883–3894, New York, NY, USA, 2016. Association for Computing Machinery.