

Frictions in applying anthropological methods to investigate cyber-insecurity among marginalised users: a case study of indigenous people in Ecuador

Alexander Kopsch
University of Bristol

Kopo M. Rampokapane
University of Bristol

1 Introduction

Using social science methods in cybersecurity research can create frictions due to the incongruence between the objective of sharing highly detailed qualitative research on one hand and the sensitive nature of cybersecurity on the other. For example, security researchers examining the security practices of activists in Hong Kong had to consider how much data to publish, since detailed knowledge of those practices could be used to harm participants [1]. This illustrates a broader tension within interpretive research; it offers a rich, contextualised account of social life [5], yet in security contexts such detail may increase the possibility of harm to participants. As usable security and privacy research increasingly engages with non-Western and marginalised groups [14, 19, 20], we need more discussions around the challenges of using qualitative methods in ways that preserve both analytical richness and participant safety.

The purpose of this workshop paper is to share the frictions (ethics and expectations) we encountered in applying anthropological research methods to security research with a specific type of marginalised user group, Indigenous Peoples. To do so, we use notes from a reflective log we held during fieldwork on cyber-insecurity of indigenous people in Ecuador. Our key takeaway is that we need to establish guidelines for best research practices with marginalised groups.

2 Context

We conducted a study on cyber-insecurity and indigenous people in Ecuador. Ecuador has a relatively high indigenous population that actively uses digital technologies, but their digital risks are not being researched [7, 10, 11]. We used interviews (16), workshops (4) and fieldnotes, inspired by a multi-sited ethnographic approach [9], with 89 participants.

Scoping trip. We prefaced our study with a scoping trip to the country. Anthropologists contend that qualitative research should be grounded in the voices of the participants [6], and,

because cybersecurity literature engages little with Indigenous Peoples, we first needed to understand what participants themselves considered important to research, and how such research should be conducted.

Reflective log. During our fieldwork, we also held a reflective log. In this reflective log, we captured how we might have influenced the field, and what kinds of problems we encountered. Noting down reflections is a common practice in anthropological research [4]. The reason behind using a reflective log is that qualitative research such as ethnography actively acknowledges the situated nature of scientific knowledge, meaning, that a researcher’s persona can have a significant impact on data collection and analysis [17].

3 Dilemmas

Dilemmas can emerge when studying the cybersecurity of Indigenous peoples, because western scientific research practices can stand in conflict with indigenous ways of knowing and reinforce colonial power dynamics, but there is little guidance on addressing this problem in cybersecurity [12, 15].

3.1 Dilemma 1: When ethics aren’t enough

Reciprocity. A particular ethical issue we encountered in our research was reciprocity. Research with marginalised populations shows that a majority of cybersecurity studies provide monetary compensation to participants [14]. However, debates in anthropology argue that financial payments can stand in contradiction to the foundations of many indigenous societies that are not based in capitalism [13, 18]. We felt:

“Reciprocity is such a huge issue for me, and it’s breaking my head, because I can’t find any similar research that gives practical advice on which types of reciprocity are appropriate, and when I ask [indigenous] leaders, they don’t tell me either.” (Notes from reflective log, September 2025)

Extractive research practices. The issue of compensation was further complicated by the issue of extractive research practices, which are a common and shared history of Indigenous Peoples engaging with academics [15]. We encountered the concern with extractivism multiple times ourselves. For example, a participant mentioned that:

“But there is a lot of jealousy now, jealousy to share, no? Information or of asking what you will do with

this [knowledge], because we come from a past in which, like how you are interviewing me right now, and then I will never hear from you again (laughs)." (Participant 21)

We later reflect on this comment:

"she made a parallel between myself and the extractivist practices of researchers before me. And it hurts and I feel guilty, even though I am trying my best to give back and be reciprocal. But I have no idea how [...]" (Notes from reflective log, December 2025)

Little guidance. To our knowledge, there is no established code of ethics for doing academic research in cybersecurity. There is the Code of Ethics by the Association for Computing [2], as well as the Menlo report [3], and also ethics boards at universities, but none of these sufficiently target the types of ethical dilemmas cybersecurity academics are faced with [8]. This inadequacy of ethics guidelines in cybersecurity is even more accurate when researching disadvantaged groups.

Summary. We encountered three ethical frictions:

1. Financial vs. culturally appropriate reciprocity.
2. Avoiding extractive academic practices.
3. Lack of guidance by cybersecurity ethics codes.

3.2 Dilemma 2: Expectations

Language. Another point of friction for us was on using the right terms to speak with participants about cybersecurity. Indigenous groups in Ecuador are often excluded from capacity-building activities and thus do not use terms like cybersecurity or privacy in their daily lives. However, there is an expectation for ethnographers to use the language of the participants [16]. Consequently, we struggled to find ways to frame interview questions:

"In terms of interviews, the first few were very tough, as I needed to find out the appropriate language and types of questions to ask the participants. They were not really speaking about digital threats or technologies, or it was very short, and they talked about other topics at length. While I tried to keep the thematic blocks the same [...], I needed to adjust the questions through trial and error [...]" (Email exchange between the researchers, October 2025)

Foregrounding participant voices. Apart from the need to adapt interviewing techniques, we also struggled with negotiating our roles. Workshop participants often expected us to teach them about cybersecurity, however, since the interpretive turn in anthropology, there is an agreement that

ethnographic research should allow participants to speak for themselves [6]. That is, we had to negotiate the expectations of participants of us as teachers, but also not subjecting them to our own notions of security. In our reflective log, we noted:

"This brings me to the next issue: How do you talk about cybersecurity or threats with people who are unfamiliar with the terms and moreover, with the ideas of technologies. I did a lot of thinking about how I should get people talking about digital threats without making this a security talk where I'm teaching them something." (Notes from reflective log, September 2025)

Summary. We experienced a conflict of expectations:

1. Using appropriate language in interviews, but participants unfamiliar with cybersecurity term.
2. Participants saw us as teachers, but we wanted to foreground their own words.

4 Key takeaway

Applying anthropological research methods to study Indigenous Peoples' cyber-insecurity creates frictions, which impact the research process and create additional challenges that need addressing. We endeavoured to abide by anthropological principles, like, avoiding extractive research, letting participants speak for themselves, and tailoring the research to their needs, but found it difficult due to a lack of guidance by ethics boards in cybersecurity and the relative novelty of the term 'cybersecurity'. Though we addressed tensions of participant and academic expectations through trial and error, iteratively reflecting on and refining interviewing techniques and workshops, an open question remains whether we succeeded in reciprocating the help of participants in a meaningful way.

Implication. We need to establish best practices for aligning qualitative cybersecurity research with social science perspectives, such as those in anthropology regarding Indigenous Peoples and ethnography. However, the risks of standardising such qualitative methods must also be discussed further.

5 Conclusion

In this short workshop paper, we have shared our experiences of applying anthropological methods and viewpoints to cybersecurity research with a marginalised user group. Using notes from a reflective log we held during ethnographic-style research with indigenous people in Ecuador, we have discussed dilemmas of ethics and expectations. These dilemmas have come up due to the epistemological and ontological tensions between the two disciplines and a lack of guidelines. Therefore, we have argued that we need to establish best practices for this type of interdisciplinary research.

References

- [1] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in Large-Scale urban protests: the case of hong kong. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3363–3380. USENIX Association, August 2021.
- [2] Association for Computing Machinery. ACM Code of Ethics and Professional Conduct. <https://www.acm.org/code-of-ethics>, 2018.
- [3] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The Menlo Report. *IEEE Security & Privacy Magazine*, 10(2):71–75, March 2012.
- [4] Robert M. Emerson, Rachel I. Fretz, and Linda L. Shaw. *Writing Ethnographic Fieldnotes*. Chicago Guides to Writing, Editing, and Publishing. The University of Chicago Press, Chicago, 2nd ed edition, 2011.
- [5] Clifford Geertz. *The Interpretation of Cultures: Selected Essays*. Basic Books, Inc., New York, 1973.
- [6] Tanya M. Luhmann. Thick Description: Methodology. In *International Encyclopedia of the Social & Behavioral Sciences*, pages 291–293. Elsevier, 2015.
- [7] Pascal Lupien. Indigenous Movements, Collective Action, and Social Media: New Opportunities or New Threats? *Social Media + Society*, 6(2):1–11, April 2020.
- [8] Kevin Macnish and Jeroen Van Der Ham. Ethics in cybersecurity research and practice. *Technology in Society*, 63:101382, November 2020.
- [9] George E. Marcus. Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography. *Annual Review of Anthropology*, 24:95–117, 1995.
- [10] Cheryl Martens, Etsa Franklin Sharupi Tapuy, and Maria de-los Angeles Ortega-Calle. Decolonizing AI rationality in the Ecuadorian Amazon. *Globalizations*, pages 1–18, November 2025.
- [11] Cheryl Martens, Cristina Venegas, and Etsa Franklin Salvio Sharupi Tapuy, editors. *Digital Activism, Community Media, and Sustainable Communication in Latin America*. Springer International Publishing, Cham, 2020.
- [12] Gabriel Tuhafeni Nhinda and Fungai Bhunu Shava. Towards the use of Participatory Methods in Cybersecurity research in rural Africa: A grassroots Approach. In *2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pages 1–7, November 2021.
- [13] Amanda Sabin. Prioritizing Indigenous Participation and Compensation in Research. *Journal of Critical Global Issues*, 1(1), February 2024.
- [14] Shruti Sannon and Andrea Forte. Privacy Research with Marginalized Groups: What We Know, What’s Needed, and What’s Next. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):455:1–455:33, November 2022.
- [15] Linda Tuhiwai Smith. *Decolonizing Methodologies: Research and Indigenous Peoples*. Zed, London, third edition edition, 2021.
- [16] James P. Spradley. Asking descriptive questions. In *The Ethnographic Interview*, pages 44–61. Wadsworth, Belmont, Calif, reprint edition, 2011.
- [17] Thomas Stodulka. Fieldwork, Ethnography, and Knowledge Construction. In Lene Pedersen and Lisa Cliggett, editors, *The SAGE Handbook of Cultural Anthropology*, The SAGE Handbook of the Social Sciences, pages 99–118. SAGE, Los Angeles, 2021.
- [18] J. L. Trotti. Compensation versus colonization: A common heritage approach to the use of indigenous medicine in developing Western pharmaceuticals. *Food and Drug Law Journal*, 56(3):367–383, 2001.
- [19] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies, COMPASS ’18*, pages 1–14, New York, NY, USA, June 2018. Association for Computing Machinery.
- [20] Yang Wang. The Third Wave? Inclusive Privacy and Security. In *Proceedings of the 2017 New Security Paradigms Workshop, NSPW ’17*, pages 122–130, New York, NY, USA, October 2017. Association for Computing Machinery.