Tensions and frictions in researching activists' digital security and privacy practices

Maya Indira Ganesh
Director of Applied Research
Tactical Technology Collective
maya@tacticaltech.org

Becky Kazansky
Lead Programme Researcher
Tactical Technology Collective
beckyk@tacticaltech.org

Jeff Deutch
Programme Researcher
Tactical Technology Collective
jeff@tacticaltech.org

1. OVERVIEW

Tactical Tech is a practitioner NGO working on digital security and privacy, with deep connections to activist communities around the world. This puts us in a unique position to do qualitative research to learn about the impact and efficacy of our work, and to document how different activist communities adopt digital security and privacy practices (or don't). However, research in digital security and privacy training environments can be riddled with ethical and practical challenges. This talk will surface the tensions that have arisen for us as researchers and activists through projects on a range of issues around privacy and security in rights-based activist and advocacy communities.These questions and tensions are about methodological approaches, and ethics in framing issues and practices. This proposal is an opportunity to speak to a research community about the limits and opportunities for research, methods and approaches and to ask how activist practices and spaces become research sites whilst being mindful of the risks to communities we work with.

2. TACTICAL TECH'S CONTEXT

2.1 About Tactical Technology Collective

Tactical Technology Collective ('Tactical Tech') is an international organisation that is committed to the use of information in activism. Based in Berlin, we work with an international network of partners and collaborators to help rights, accountability and transparency advocates and the communities they work with to use information and digital technologies effectively in their work. We have three focal areas: 'understanding & shaping issues; digital security and privacy; and data politics [1]. We work to raise awareness, build practical skills and offer critical reflection and inspiration in all of these areas.

2.2 Building Digital Security and Privacy Capacity

For over ten years Tactical Tech has supported human rights defenders, (HRDs) activists, journalists, bloggers and transparency advocates to use digital technologies safely and securely. These activists face risks associated with mass and targeted surveillance; restrictions on freedom of speech, movement and assembly; and threats emerge from state and non state actors alike. We do digital security trainings through intensive, small workshops; post-trainings we maintain contact with our trainees through closed group lists. Our online resource Security in a Box, currently available in 15 languages, has received 2.7 million visitors a year for the past two years. In addition to digital security and privacy trainings, our work has been enthusiastic about the opportunities for 'information activism'; much of our early work was based on enabling activists to tap the potential for information and digital technologies to expose corruption, violence and injustice through artful and creative methods. This engagement with communities has given us a rich appreciation of how activists use and work with technologies, and what the limits to it are. More recently, we've become far more aware of how the use of technology in activism can put activist users at risk, particularly in light of the Snowden Leaks, and governments' increasing investment in surveillance technologies and targeting of activists. In response to the changing nature of threats to activists, our emphasis with our Exposing the Invisible project [2] is to support investigative and aesthetic practices with journalists, citizens, artists, technologists and hackers safely and securely.

2.3 Current Research

In the past 18 months we've started closely documenting and learning about and from our work. We have three broad areas of focus at present. First, we're exploring digital security capacity building work and activist practices to understand the ways in which digital security and privacy practices are enabled and sustained in complex, shifting, geopolitical and activist contexts. This work also makes a case for why security and privacy education must be understood in context Second, a study in two countries on the flip sides of technologies for transparency and accountability, and how these technologies may pose security and privacy risks to activists who are marginal in their societies. Third, we're training women journalists, activists and HRDs to become confident as privacy advocates and as digital security trainers. Our research in this area will be more evaluative to understand the effects of supporting a global advocacy and activist community.

3. DO NO HARM

Do no harm' [3] is a principle that has become an important guiding aspect of our work. Simply put, 'DNH' acknowledges that interventions from the outside affect local situations. In an environment where the use of privacy enhancing technologies is being criminalised [4], we have to be conscious of our role in promoting materials and tools that may implicate activist communities. This has already happened with the citing of Security in a Box in the case of the arrest of the Zone 9 Bloggers in Ethiopia[5]. Whilst NGOs may not have formal ethical review board processes, principles like Do No Harm can serve as a powerful tool which which to think about practices and process of research. It begins by asking, simply, what the potential sources and points of harm are for a marginal, and possibly traumatised, community. Part of this includes ensuring that research is conducted in an environment where respondents feel safe and secure, and where steps are taken to ensure that meeting with respondents poses as little additional risk to partner communities as possible. Another important part of this is to operationalise practices that ensure the security and confidentiality of the research, starting from the planning phase through its publication.

This includes conducting research discretely in communities, ensuring the security of research materials, and anonymizing findings in a way that honors specificity while removing information that can expose communities. However, Do No Harm can also set limits that could make research very difficult or almost impossible due to the potential risk of exposure to respondents.

4. TENSIONS AND FRICTIONS IN ACTIVIST RESEARCH ON DIGITAL SECURITY AND PRIVACY

Anna Tsing's work [6] on frictions and global connections provides a way to start thinking about tensions in doing research as privacy advocates with activist communities. 'Tension's are fairly well understood as limitation or hurdles. Her work allows for "tension's counterpart", friction, to emerge. She writes: "[a]s a metaphorical image, friction reminds us that heterogenous and unequal encounters can lead to new arrangements of culture and power...Friction inflects historical trajectories, enabling, excluding, and particularizing." Friction is a force between surfaces what actually makes movement possible; in a sense, friction may even be a positive or constructive force. Tsing draws on studies of political and social movements, and suggests that risks, limitation and impediments often have a counterpart-friction – that makes motion possible. Just as surface tension and friction enable movement in the physical world, tensions offer opportunities for productive movement -friction. A 'friction' may present as an opportunity for a new intervention, tactic, partnership, education strategy, collaboration etc. Identifying and acting on moments of friction to create something tangibly positive for research respondents could be an important way to work through the tensions.

Ethnographic and action research studies in the development of security and privacy practices, and the risks and barriers to it, are scarce, as is the literature on the effects of surveillance on HRD and activist groups' work in different parts of the world. Thus there is scant discussion of the practical, ethical and methodological issues in doing this work. Our recent projects have surfaced of points of tension that we present here for further discussion.

4.1 Responsibilities of the activist-researcher

In our research projects we ask respondents to talk about their digital practices. In a study of risks and barriers to technology use perceived by vulnerable activists in an African country, respondents described struggling with managing their social media profiles and the fear of lateral surveillance. As researchers who are also knowledgeable about digital security and privacy enhancing practices, the instinct to correct, supplement or add to respondents' understanding and practices is a source of struggle. Being known as an organisation that provides practical support and training, not doing so is sometimes confusing for respondents who expect us to. In one case we were expressly asked (by an academic partner) not to mention that we could offer digital security and privacy trainings or inputs for how it could be leading, or seem as an exchange for time spent as a research respondent. At the same time, we have a moral imperative to support people that we find asking for it. One tactic we used in the African case study was to use the interview setting to collect information, and to provide materials and resources to respondents *after* the research had been completed.

A Do No Harm framework means that activist-researchers must constantly work to minimise possible negative repercussions from their work, both in the research process and presentation of findings. Collecting stories of harm is often needed, or so it is imagined, in order to make a legal case against surveillance, or to document that surveillance is occurring. However in doing so, researchers can put respondents at risk of exposure by publishing reports with details that identify them. It can be difficult to make such arrangements beforehand, but where possible measures to ensure the safety of respondents can be planned.

When applied research is, itself, an intervention, we face challenges of ensuring that the research being conducted is sound and that we are not introducing bias or leading respondents to a particular answer or solution. When interviewing respondents on risk or threat perception, for instance, we are faced with a dilemma of correcting respondents whose perceptions are misinformed and not correcting respondents which may leave respondents in a heightened psychosocial state. These challenges led us to ask questions about the infrastructure and resources for research on privacy and security in at-risk and marginal communities. If action research is a feasible option, then that needs to be built into project design. We see this as productive *friction*.

As activist-researchers, we may insist on not documenting events or trainings through film and photography for reasons of privacy, however documentation may mean something entirely different for the sociality of participants or for those respondents who organise events locally. In a recent review of digital security interventions in three African countries, we found that digital security trainings act not only for their intended purpose of skill-sharing, but also as a spaces of contact and networking for activists in a given region. In a recent event with women activists, we organised a group photograph but asked respondents to choose different, creative ways to obscure (or reveal) themselves. The act of visual documentation can also be a moment to discuss the risks and mitigation strategies associated with it.

When presenting research findings in a Do No Harm framework, activist-researchers continually face challenges of de-identifying respondents to mitigate risk while still being able to introduce context and nuance in discussing themes. In the Security in Context research, we aggregate findings and talk about at least two groups with common experiences, so as to lessen the chances of identifying a specific group or individual.

Thus, in researching activists' digital security and privacy practices it becomes important to envisage the tensions and identify opportunities for productive and creative responses.

5. REFERENCES

[1] More about our work can be found at tacticaltech.org.

[2] See exposingtheinvisible.org.

[3] Anderson, M.B. 1999 *Do No Harm: How Aid Can Support Peace – or War.* Lynne Rienner Pub.

[4] Riseup. 2015 https://help.riseup.net/en/security-not-a-crime.

[5] Tactical Technology Collective and Frontline Defenders 2014 https://tacticaltech.org/news/tactical-techs-and-front-line-defenders-statement-zone-9-bloggers..

[6] Tsing, A. 2005. *Friction: An Ethnography of Global Connection.* Princeton University Press: Princeton, NJ