

Adversarial Participatory Research: A research method for tackling ethico-technical dilemmas

Lisa Geierhaas
University of Bonn

Matthew Smith
University of Bonn, Fraunhofer FKIE

Abstract

This extended abstract proposes Adversarial Participatory Research (APR) as a methodology for studying complex, contested ethico-technical dilemmas such as found in the surveillance vs privacy debate. These debates often combine ethical disagreement, technical uncertainty, institutional mistrust, and competing rights, such as privacy, security, public safety, and protection from harm [23]. APR addresses this complexity by involving opposing stakeholder groups directly in iterative, evidence-based research cycles. The aim is to make ethical assumptions explicit, separate ethical from technical disagreements, and translate areas of agreement into actionable requirements for technology, policy, and legislation.

1 Introduction

Computing professionals and tech companies frequently design systems with substantial societal impact. In the security and privacy (S&P) domain, ethical dilemmas are especially prominent, touching on issues such as government surveillance, corporate tracking, parental monitoring, content filtering, civil liberties, free speech, and online harassment. Many of these S&P topics are particularly challenging because they contain a complex mix of ethical and technical issues [23].

One prominent example is the “Crypto Wars” [18], the long-running conflict between government authorities and privacy advocates regarding encryption and surveillance technologies. The debate intensified after the Snowden revelations [25] and continues in controversies surrounding Client-Side Scanning (CSS) [2, 16].

The EU [1] states: “*The European Convention on Human Rights protects the right to respect for private life, the home and correspondence. This includes protecting the privacy of messages, phone calls, and emails. Governments can only interfere with these rights when it is specifically allowed by law, and done for a good reason – like national security or public safety.*” The ethical dilemma lies in balancing competing goods such as privacy, child protection, public safety, and civil liberties.

Current state-of-the-art research methodology in the field of human factors of S&P / Usable Security and Privacy (USP) and Behavioral Ethics (BE) while excellent in their respective fields are not optimal to study the complex interplay of these ethico-technical dilemmas [23]. Each of the sub-fields has its unique view on S&P but they are all missing key elements to make progress. BE is well-suited to studying isolated ethical dilemmas [3, 19]. USP is well-suited to studying isolated socio-technical topics [9, 11, 15, 20, 21]. participatory research (PR) is excellent for understanding disadvantaged groups and creating positive actions with and for them [4, 27]. adversarial collaboration (AC) is great for solving disputes between researchers [6, 13]. None of these on their own is well-suited to tackle the complex and adversarial landscape of ethico-technical dilemmas in S&P.

The typical procedure for both qualitative and quantitative studies is that researchers design a study and run it with a sample of participants who, once completed, are not involved in the research further. The study durations are also usually fairly short. At SOUPS 2023 the mean time for interviews was 55 minutes (SD=21) and for surveys, the mean time was 13 minutes (SD=7). Maesschalck [19] states: “*The typical research designs used in behavioral ethics research require such a reduction of complexity that the resulting findings are not very useful for practitioners.*”

Both the linear nature and short contact time hinder the current methodology when tackling multi-faceted, complex, and adversarial dilemmas. To address this, we propose APR, a methodology combining PR, AC, and grounded theory (GT) [5]. APR is designed to disentangle complex ethical

and technical dilemmas while fostering trust and collaboration in adversarial settings.

2 Background & Related Work

APR is a combination of methodologies from several related fields. It combines PR [4, 27], AC [6, 13], and GT [5], to disentangle complex ethical and technical dilemmas while fostering trust and collaboration in adversarial settings.

PR is a research-to-action method that actively involves the people who are the subject of the study in the research process itself [7]. It is a very heterogeneous research method. In their overview, Vaughn et al. identified 26 distinct versions of PR [27]. It has also been applied to a wide variety of areas with a particular focus being on disadvantaged groups [8] and healthcare [4]. To ascertain the prevalence of PR at top-tier S&P venues, we analysed all papers published between 2019 and 2025 at IEEE S&P, ACM CCS, Usenix Security, NDSS, Crypto, CHI and SOUPS. In over 4000 papers, we only found a few instances where PR was used. Like above, it was mostly used to better understand at-risk groups, e.g., children [14, 17].

A similar picture presents itself in the BE community. In a literature review covering the past five years, we found only a handful of papers suggesting the use of PR but no instances of it actually being used [12, 22, 24, 26, 28]. As above, the main benefit seen in PR is the ability to understand and create positive change for disadvantaged groups [4]. Another feature of PR is the sense of agency and trust in the data that participants gain. However, to unlock this potential, PR needs to be extended and fused with AC to encompass the adversarial nature of the ethico-tech dilemmas.

Adversarial Collaboration [6] has not received much attention despite some high-profile researchers like Kahneman championing it [13]. In AC, disagreeing scholars (not study participants) work together to test their competing hypothesis [6]. We did not find any evidence of AC being used in S&P, USP or BE research.

We also could not find any prior work fusing PR and AC to tackle ethical dilemmas. We are hopeful that this fusion will offer a new and more productive method for tackling ethico-technical dilemmas.

3 Adversarial Participatory Research

The APR process begins with researchers discussing the current state of an ethico-technical dilemma with a stakeholder group. In the case of CSS [2], this could include privacy activists, Computer Science (CS) students, law enforcement officers, or Cybercrime Investigation (CCI) students. Some prior studies have triggered methodological objections such as framing bias or claims that researchers are “*asking the wrong question*” [10]. APR addresses this by co-designing new qualitative, quantitative, or mixed-methods studies together with

participants. Researchers execute and analyze the studies, and findings are discussed again with the stakeholders.

The adversarial component emerges by integrating opposing groups into the process. Research cycles initially run in parallel, allowing different “sides” to present evidence and challenge one another using scientifically grounded data. Once disagreements or unresolved questions are identified, stakeholders jointly agree on study designs that can address those points of contention. This process transforms adversarial debates into collaborative evidence generation.

APR further incorporates theoretical sampling from GT [5]. New stakeholder groups can be added when debates require additional expertise. For example, if participants challenge the claim that investments in social services could reduce online abuse, social workers or policymakers can be recruited into the process. Dynamic regrouping also enables researchers to cluster participants by variables such as trust in government, support for surveillance, or ethical framework, rather than simplistic pro- or anti-surveillance labels. This means that the exact stakeholder groups that are involved in the process are not decided by the researchers alone, but are influenced by the perspectives and the feedback of already involved groups.

The central hypothesis of APR is that explicitly disentangling ethical and technical aspects will reduce adversarial conflict and increase support for jointly developed proposals.

To get a first assessment of the feasibility of APR, we conducted two scaled-down four-month dilemma studies. In the first, we used a basic PR (not APR) approach with 75 S&P CS master students from our security lecture, two ethics faculty, and a police officer from an Online Child Abuse Investigation Team. Here, we would consider the adversarial groups to be the students, whose IT security background makes them largely opposed to digital surveillance measures, and the police, who see some of these measures as a necessary tool for their work. At the end of the test run, we retained all experts and 44 of the original 75 participatory CS students, which was more than sufficient for our purpose, which was to design a study that would probe into the acceptability of certain digital surveillance measures. We recruited an additional 73 S&P CS bachelor students and 15 CCI students. In the second study, we recruited 61 CS students and retained 57 after four months and 6 studies. The interest, engagement, and trust in the results were excellent and exceeded expectations, suggesting that stakeholders are willing to engage productively despite holding opposing views. This suggests to us that APR is a promising approach to reshape how the human aspects of surveillance and privacy conflicts are researched. Beyond producing more trusted and ethically grounded proposals in S&P, APR could also provide a generalizable framework for studying adversarial ethico-technical dilemmas [23] across many domains. By transforming “crypto wars” into collaborative efforts to resolve the “crypto dilemma,” APR offers a pathway toward more productive, evidence-based, and less polarized debates.

References

- [1] Right to privacy - Impact of the European Convention on Human Rights - www.coe.int.
- [2] Ross Anderson. Chat Control or Child Protection, 2022.
- [3] Max H. Bazerman and Francesca Gino. Behavioral Ethics: Toward a Deeper Understanding of Moral Judgment and Dishonesty. *Annual Review of Law and Social Science*, 8(1):85–104, December 2012.
- [4] Margaret Cargo and Shawna L. Mercer. The Value and Challenges of Participatory Research: Strengthening Its Practice. *Annual Review of Public Health*, 29(1):325–350, April 2008.
- [5] Kathy Charmaz. *Constructing Grounded Theory*. SAGE Publications Ltd., March 2024.
- [6] Cory J. Clark and Philip E. Tetlock. Adversarial Collaboration: The Next Science Reform. In Craig L. Frisby, Richard E. Redding, William T. O’Donohue, and Scott O. Lilienfeld, editors, *Ideological and Political Bias in Psychology: Nature, Scope, and Solutions*, pages 905–927. Springer International Publishing, Cham, 2023.
- [7] Andrea Cornwall and Rachel Jewkes. What is participatory research? *Social Science & Medicine*, 41(12):1667–1676, December 1995.
- [8] Denise De Las Nueces, Karen Hacker, Ann Di-Girolamo, and LeRoi S. Hicks. A Systematic Review of Community-Based Participatory Research to Enhance Clinical Trials in Racial and Ethnic Minority Groups. *Health Services Research*, 47(3pt2):1363–1386, 2012. [_eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1475-6773.2012.01386.x](https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1475-6773.2012.01386.x).
- [9] Francesco Di Nocera, Giorgia Tempestini, and Matteo Orsini. Usable Security: A Systematic Literature Review. *Information*, 14(12):641, December 2023. Number: 12 Publisher: Multidisciplinary Digital Publishing Institute.
- [10] Lisa Geierhaas, Florin Martius, Arthi Arumugam, and Matthew Smith. “Not the Right Question?” A Study on Attitudes Toward Client-Side Scanning with Security and Privacy Researchers and a U.S. Population Sample. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 2246–2263, San Francisco, CA, USA, May 2025. IEEE.
- [11] Matthew Green and Matthew Smith. Developers are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security & Privacy Magazine*, 14(5):40–46, 2016.
- [12] Virgil L. Gregory. Cognitive-behavioral group therapy and buprenorphine: Balancing methodological rigor and community partner ethical concerns in efficacy-effectiveness trials. *Ethics & Behavior*, 30(5):364–384, July 2020.
- [13] Daniel Kahneman and Gary Klein. Conditions for intuitive expertise: A failure to disagree. *American Psychologist*, 64(6):515–526, 2009.
- [14] JaeWon Kim, Robert Wolfe, Ramya Bhagirathi Subramanian, Mei-Hsuan Lee, and Jessica Colnago. Trust-Enabled Privacy: Social Media Designs to Support Adolescent User Boundary Regulation. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, 2025.
- [15] Tadayoshi Kohno, Yasemin Acar, and Wulf Loh. Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations. pages 5145–5162, 2023.
- [16] Ian Levy and Crispin Robinson. Thoughts on child safety on commodity platforms, July 2022. [arXiv:2207.09506 \[cs\]](https://arxiv.org/abs/2207.09506).
- [17] Lanjing Liu and Yaxing Yao. From Knowledge to Practice: Co-Designing Privacy Controls with Children. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI ’25, pages 1–22, New York, NY, USA, April 2025. Association for Computing Machinery.
- [18] Kevin Macnish. An End to Encryption? Surveillance and Proportionality in the Crypto-Wars.
- [19] Jeroen Maesschalck. Making Behavioral Ethics Research More Useful for Ethics Management Practice: Embracing Complexity Using a Design Science Approach. *Journal of Business Ethics*, 181(4):933–944, December 2022.
- [20] Bryan D. Payne and W. Keith Edwards. A Brief Introduction to Usable Security. *IEEE Internet Computing*, 12(3):13–21, 2008. Publisher: IEEE.
- [21] M. Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. Debunking Security-Usability Tradeoff Myths. *IEEE Security & Privacy*, 14(5):33–39, September 2016. Conference Name: IEEE Security & Privacy.
- [22] Julia Slupska. Networks of Care: Tech Abuse Advocates’ Digital Security Practices.
- [23] Matthew Smith. The Opposing Side Is Not the Enemy: From Socio-Technical Debates to Ethico-Technical Deliberations in Security, Privacy, and AI. 2026.

- [24] Ruth G. St. Fleur and Seth J. Schwartz. Increased research literacy to facilitate community ownership of health research in low and middle income countries. *Ethics & Behavior*, 30(6):414–424, August 2020.
- [25] Susan Landau. The Second Crypto War - What's Different Now. 2018.
- [26] Eli Talbert. Beyond Data Collection: Ethical Issues in Minority Research. *Ethics & Behavior*, 29(7):531–546, October 2019.
- [27] Lisa M. Vaughn and Farrah Jacquez. Participatory Research Methods – Choice Points in the Research Process. *Journal of Participatory Research Methods*, 1(1), July 2020.
- [28] David Wasserman. A Case for Greater Risk Tolerance in Internet Use by Adults with Intellectual Disabilities: A Comment on Chalghoumi et al. *Ethics & Behavior*, 29(3):223–226, April 2019.