Poster: Unintended Consequences of Security and Privacy Software

Harshini Sri Ramulu
The George Washington University
sriharshini@gwu.edu

Yasemin Acar
The George Washington University
acar@gwu.edu

***Abstract*—Security and privacy software is being created to have positive impacts on people, e.g., to protect them from surveillance and keep them safe. However, there may be negative unintended impacts by the wide distribution of this software. We do not currently know how this is being mitigated, and if unintended negative consequences are systematically being prevented. While there are several ethics impact frameworks for developers to use to work through ethical and societal impacts, it is currently not known if these are widely known and/or used in a structured way for security and privacy software. In this paper, we investigate the awareness and attitudes of developers of security and privacy software towards issues addressed in frameworks for ethical and societal impacts. We used eight such frameworks to identify intended and unintended consequences that should be considered during the development process. Based on these topics, we developed a semi-structured interview guide, and are currently conducting an interview study with S&P developers of software, such as encrypted email, secure messaging, and private browsing. Preliminary results show that developers lack awareness of mitigating unintended consequences systematically, have considered incomplete subsets of societal impacts, but are generally positive and open to learning about impacts, and considering these going forward. We recommend broader awareness of the issues addressed in ethical frameworks, for example by considering them in education, developer resources, and including them in regulation.**

I. Introduction

Developers of security and privacy enhancing software impact lives of a plethora of people in a profound number of ways. Security and privacy software specifically are aimed at creating a positive impact on society by protecting users from vulnerabilities, protecting their data privacy, keeping their communication confidential etc. However, while created to protect people, this software may be prone to unintended consequences that raise ethical concerns due to the wide distribution of these products.

For instance, encrypting email can be a daunting task for a majority of users because it involves various steps like the receivers installing software and verifying keys, making the process very tedious [1]. Users may inadvertently lose access to their emails if they lose their private keys. Authentication tools may be inaccessible to people with visual impairments, because these mechanisms have not been designed with these users in mind [2]. Secure messaging applications can pose risks of misinformation being forwarded [3]. Creators of software often do not involve their users during the development process nor assess the worst possible impact of their software [4]. Not considering diverse accessibility needs can exclude or make software harmful to users with disabilities, children, older adults, activists, non-western populations, victims of domestic violence, etc. [5]

The Human Computer Interaction (HCI) and Artificial Intelligence (AI) communities have explored numerous ethics frameworks to assess and minimize these unintended consequences. Additionally, participatory design models have been proposed to work with dis-empowered communities to articulate and address their concerns with technology. Resources and frameworks like the Ethical OS toolkit [6] and Digital Impact tool kit [7] help assess the impact of digital technology. Several aspects like misinformation, inequalities, biases, addiction, accessibility, surveillance, risks by criminal actors, etc., are addressed in these frameworks [8]–[13]. These should help organizations introspect about the unintentional harms that might arise due to the use of their software.

It is currently unclear whether security and privacy software developers are aware of these frameworks, and/or the themes discussed in these frameworks, and whether they address them in a systematic way during development. Therefore, in this study, we aim to understand how developers of security and privacy software address ethical issues. Additionally, we also want to understand the attitudes and perceptions of security and privacy software developers towards negative consequences of their software. This study addresses the following research questions:

1) What is the awareness and attitudes of security and privacy (S&P) software developers with respect to the ethical and societal impacts of security software?
2) What are S&P software developers' experiences with societal impact / ethics resources, frameworks and tools? (How) do they use them, if at all?

II. Approach

To answer our research questions, we conduct semi-structured interviews with stakeholders of security and privacy software. We choose this approach due to the exploratory nature of our study. During the interviews, developers are asked about their experiences, and we can explore in-depth with follow-up questions. The goal of this ongoing study is to interview a diverse set of developers of software designed to create a positive impact by improving security and privacy.

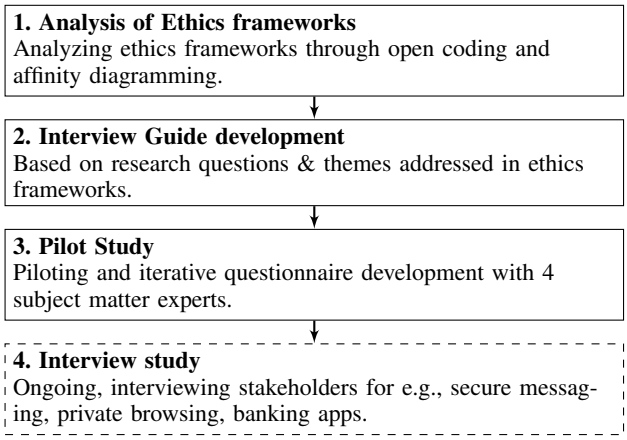

Fig. 1. Overview of our study methodology.

Ethics Framework analysis: In our interview guide, we include themes covered in frameworks that focus on the potential negative or unintended harm that can be caused by technology. To develop a comprehensive view of these aspects, we analyzed eight frameworks developed in different fields. We used a digital collaborative whiteboard to open code and affinity diagram the themes that that are discussed in these frameworks. The categories created by the lead author were verified and discussed with the other author. These categories inform our interview guide.

Interview Guide Structure: Our interview guide asks participants questions in three general areas: (1) *awareness of their user-base*, (2) the potential *unintended consequences* they anticipate through the use of their software, and (3) their *awareness and experiences with ethics*.

Pilot study: We piloted our interviews to evaluate the validity, comprehensibility and language of the interview questions. We conducted four pilots, two with professional colleagues not involved in this project, and two with developers from another industry. We iterated our interview guide based on the pilot interviews and participant feedback, mostly for comprehension, question order, and to add examples.

Ethical Consideration: This study was approved by our University's Institutional Review Board (IRB). Participant data were de-identified. We only collected their email addresses if they opted-in to receive a $80 gift voucher for their participation, or if they wanted to be mailed a copy of our results. Apart from that, all the other data is associated with random identifiers. We made sure to reaffirm the participants that they could decline to answer questions or withdraw from the interview. We also ensured to mask details about their companies in our transcripts if they were concerned about causing harm to their employers' reputation.

Limitations: Like with any qualitative study, participant responses maybe subject to recall-, social-desirability and self-report biases. Additionally, our sample will not be representative of all of the security and privacy software. Due to the qualitative nature of the study, we cannot generalize results. We however think that our sample is diverse, and gives both a broad overview and deep insights into security and privacy software developers' awareness and behaviors concerning societal impacts and ethics of their software.

III. Preliminary results and outlook

Interviews are ongoing and we will continue to recruit participants until we reach theoretical saturation. Preliminary results indicate that teams do not systematically assess ethical concerns. Some teams tend to consider only certain aspects, but none of the developers we talked to so far mentioned that they have a systematic process or framework to assess the ethical risks. This leads to an inconsistent consideration of diverse ethical and societal impact themes. For example, some teams thought about making their solutions accessible for users with visual impairments but they did not involve them in the development process. One developer who mentioned that they worry about environmental impacts did not consider the accessibility of the software during development. All the developers we interviewed mentioned that they have never really thought about ethical consequences in a systematic manner. They expressed a deep desire in incorporating ethical assessments moving forward. We think that actively working with developers to address unintended or negative consequences can create a considerable positive impact in creating ethically sound security and privacy software.

References

[1] Mathew Green. The daunting challenge of secure email. https://www.newyorker.com/tech/annals-of-technology/the-daunting-challenge-of-secure-e-mail. Online; accessed November 8, 2021.

[2] Bryan Dosono, Jordan Hayes, and Yang Wang. {"I'm}{Stuck!"}: A contextual inquiry of people with visual impairments in authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 151–168, 2015.

[3] Caio Machado, Beatriz Kira, Vidya Narayanan, Bence Kollanyi, and Philip Howard. A study of misinformation in whatsapp groups with a focus on the brazilian presidential elections. In *Companion proceedings of the 2019 World Wide Web conference*, pages 1013–1019, 2019.

[4] Michael Dorin and Sergio Montenegro. Ethical lapses create complicated and problematic software. In *2021 IEEE/ACM 2nd International Workshop on Ethics in Software Engineering Research and Practice (SEthics)*, pages 1–4, 2021.

[5] Yang Wang. Inclusive security and privacy. *IEEE Security & Privacy*, 16(4):82–87, 2018.

[6] Institute for the Future and Omidyar Network. https://ethicalos.org/.

[7] Digital Impact Toolkit. https://digitalimpact.io/toolkit/.

[8] Ethics and Algortithms toolkit. https://ethicstoolkit.ai/.

[9] Data Ethics Framework. https://www.gov.uk/government/publications/data-ethics-framework.

[10] Europrean Commision Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[11] World Economic forum ethics for responsible AI . https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.

[12] ACM code of ethics and professional conduct. https://www.acm.org/code-of-ethics.

[13] Digital Ethics Guide for professionals of digital age. https://www.cigref.fr/wp/wp-content/uploads/2019/02/Cigref-Syntec-Digital-Ethics-Guide-for-Professionals-of-Digital-Age-2018-October-EN.pdf. Online; accessed Nov 8, 2021.