Security and Privacy Software Creators' Perspectives on Unintended Consequences

Harshini Sri Ramulu[1,2], Helen Schmitt[1], Dominik Wermke[3], and Yasemin Acar[1,2]

[1] *Paderborn University, Germany*
[2] *The George Washington University, USA*
[3] *North Carolina State University, USA*

Security and Privacy Software

Secure Messaging

VPN

Secure Browsers

Password Managers

...and many more

Protect users, guard privacy, keep communication confidential

Developers make decisions and tradeoffs, based on time, resources, knowledge and priorities.

What developers think, how they consider their users, has a high impact on their product.

Depending on developers' considerations, software can have unintended consequences (UCs).

Unintended consequences* are unforeseen outcomes of purposeful actions (development decisions)[1]

*They may be anticipated or unanticipated resulting in both positive and negative outcomes

[1] Merton, R.K. 1936, "The Unanticipated Consequences of Purposive Social Action", American Sociological Review, vol. 1, no. 6, pp. 894-904.

Unintended consequences in S&P software

Everyone is selling VPNs, and that's a problem for security

The influencer-VPN provider relationship is good for business, but not for security.

Are Private Messaging Apps the Next Misinformation Hot Spot?

Telegram and Signal, the encrypted services that keep conversations confidential, are increasingly popular. Our tech columnists discuss whether this could get ugly.

How the world's biggest dark web platform spreads millions of items of child sex abuse material — and why it's hard to stop

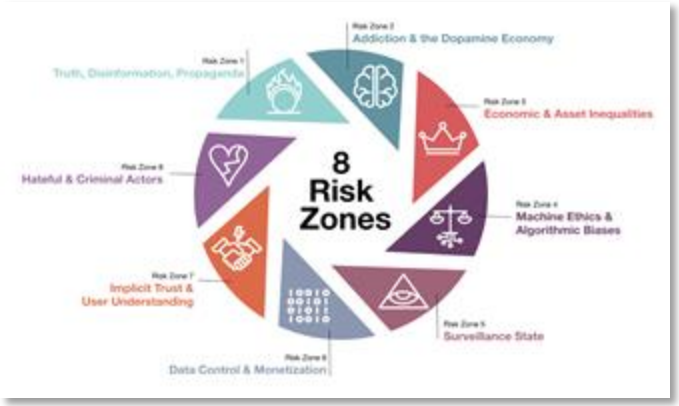
Published: September 2, 2021 4.09pm EDT

Why is encrypted e-mail so rare in the first place?

The main reason for this is as sad as it is simple: encrypting e-mail is just *hard*.

Result: Less security than intended!

Resources frameworks/ toolkits in existing literature in HCI and AI – helpful for security & privacy software?



ACM Code of Ethics and Professional Conduct

Preamble

Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. The ACM Code of Ethics and Professional Conduct ("the Code") expresses the conscience of the profession.

Guidance

Data Ethics Framework

Guidance for public sector organisations on how to use data appropriately and responsibly when planning, implementing, and evaluating a new policy or service.

Digital Impact Toolkit

Leveraging digital data in ways that advance your mission and respect the rights of the people you serve is a core capacity of foundations and nonprofits in the 21st century. That's why the **Digital Civil Society Lab** at the **Stanford Center on Philanthropy and Civil Society** created the Digital Impact Toolkit—to support civil society organizations in using digital data ethically, safely, and effectively. The content and tools on the site come from nonprofit and foundation partners.

Ethics and Algorithms Toolkit (Beta)

(Section) Part 1: Assess Algorithm Risk

Overview of toolkit beta release

Welcome to the beta release of our Ethics and Algorithms Toolkit! This toolkit is designed to help governments (and others) use algorithms responsibly.

Research Themes

Attitudes and Practices of S&P software creators concerning unintended consequences of their software

What unintended consequence of S&P software do S&P creators **anticipate**, how do they **reason about them**, and how do they **mitigate** them?

Facilitators and Blockers in considering and addressing unintended consequences

Methodology – Framework Analysis & Interviews

Interview guide

Unintended consequences probes created by analyzing ethics frameworks and toolkits from prior research

Recruitment

Through social media, personal networks, and snowballing

Interviews

N=14 Semi-structured interviews with creators of S&P software (Designers, Developers, Researchers, Executives, and maintainers)

Analysis

Inductive qualitative coding followed by thematic analysis

Findings

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

Driven by a personal motivation for “doing good”

- Intrinsic motivation to do good following own moral framework

> *“I often take it upon myself to raise concerns, especially when people start thinking about solving a problem for parents, like: ‘Oh, I want to help parents to protect or to monitor their kids’, then I have to be like, ‘They’ve got to be careful because that could be used to monitor people that are not kids or things like that’ ” - P05, Stalkerware detection*

> *“It’s not a scientific endeavor for me, I just want to do what is right in my eyes” - P04, Software release signing tool*

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

Reactive and unstructured approaches to unintended consequences

- Reactive approach relying on user feedback
- Lack of formal/ structured processes to identify negative impacts

> ***"...through feedback collection, where like we learn about the main pain points our users have and we have. Sometimes they are not easy problems to fix. They may take like a year for us to get some solution out there." - P07, Anonymity network***

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

Strong focus on improving privacy, security, and usability

- Current development practices are privacy focused and protecting from surveillance
- Usability was also sometimes mentioned

> ***"The key problem is surveillance. Corporations and states do tend to spy upon their customers and citizens" - P09, VPN***

Overlooking other harms

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

Some aspects are just not a priority (due to lack of awareness and resources)

- Accessibility was not a priority
- Access barriers for users without technical knowledge
- Disempowerment of users, disinformation, mental health impacts, biases, etc., were often not huge concerns

> ***"It is not accessibility first in general. Mainly, I would say because of a lack of specific training in the developer community towards these needs." P09, VPN***

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

Participants believe no harm is possible due to well-intentioned software

- Some negative consequences can be underestimated due to the goal of "doing good" and enhancing privacy & security

> ***"No, no, no, not at all. What we're doing here is trying to protect your system. We're trying to protect your phone from harm." - P08, VPN***

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

No control over certain aspects (Privacy-Moderation trade off)

- Some issues may surface due to lack of control and missing content moderation
- In social media tools and self-hosted software, responsibility is shifted to administrators and moderators
- Harmful actors leverage the software

"[. . .] being open source technology, privacy-first technology, it does attract certain groups which feel like anonymity gives them a space to do maybe not always lawful things right, so we did have attraction, for example, from ISIS " - P06, Social Network

"I feel that it is a little difficult to pinpoint what exactly they are using it for. But it would be naive to think that it is not used in that (harmful) way."– P07, Anonymity Network.

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

Lack of awareness at an individual and organizational level

- A shared accountability is assumed between the team members
- Strong belief that positive software can cause no harm
- Missing organizational support to speak up and mitigate ethical risks

> ***"I think it's more that we don't have the have the mandate to do it. We don't really have organizational buy-in to stop a feature from rolling out because of a perceived ethical risk. There is no one really who full-time has the job title to think about ethical issues." - P11, Browser***

Attitudes and Practices

Anticipated Consequences

Facilitators & Blockers

PROBLEMS

High ethical debt

Harms vulnerable groups by solving problems in hindsight

Security tools abandoned resulting in even lower security

Reactive approaches burdens them and puts them at risk

RECOMMENDATION

Proactively anticipate and mitigate unintended consequences

flaticon

PROBLEMS

Developers balance different roles and priorities

Lack incentives to avoid the shift of risk to users: a moral hazard problem

Lack of formal job roles and responsibilities to assess ethical and societal implications of software

RECOMMENDATION

Create incentives, official roles, and responsibilities at an organizational level

flaticon

PROBLEMS

Privacy focus may invite harmful actors to use the software

Responsibility is on self-hosters and moderators

RECOMMENDATION

Creative solutions for privacy moderation trade-off

Create trainings and guidelines for self-hosters and moderators

flaticon

PROBLEMS

Lack of systematic assessments

Reliance on personal experiences and lack of formal training

Underestimating unintended consequences because the software is developed to create a positive impact

RECOMMENDATION

Use systematic toolkits for ethical reviews similar to privacy reviews

Create ethics trainings and resources that are more prescriptive

Research Themes

1. **Attitudes and Practices** of S&P software creators concerning unintended consequences of their software
2. What unintended consequence of S&P software do S&P creators **anticipate**, how do they **reason** about them, and how do they **mitigate** them?
3. **Facilitators and Blockers** in (systematically) considering and addressing unintended consequences

Methods

Analysis of ethics and unintended consequences toolkits
14 Semi-structured interviews with creators of S&P software

Results

- Current practices are reactive
- Lack of resources and time; especially for open-source software
- Systematic frameworks are not used
- Under estimating the negative outcomes due to well intentioned nature of software
- Privacy moderation trade-off

Key insights

- Relying on user feedback burdens users; security tools abandoned resulting in even lower security
- Organizations can form
- alize ethical responsibilities in job roles
- Systematic frameworks that currently exist are not perfect but can be used as probes

Scan for paper

Harshini Sri Ramulu, Helen Schmitt, Dominik Wermke, and Yasemin Acar, ***Security and Privacy Software Creators' Perspectives on Unintended Consequences***, in *Proceedings of the 33rd USENIX Security Symposium*, August 14-16, 2024.

Contact:

Email: harshini.sri.ramulu@uni-paderborn.de

Linkedin: linkedin.com/harshinisriram

Twitter: Harshiniisriram