At-Risk Users

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

01/04/2025

THE UNIVERSITY of EDINBURGH

Overview

- At-risk users
- Revision and feedback

https://www.youtube.com/watch?v=qX5hsuH2_QM

Discuss: Who are at-risk users?

2024 IEEE Symposium on Security and Privacy (SP)

SoK: Safer Digital-Safety Research Involving At-Risk Users

Rosanna Bellini* Emily Tseng* Noel Warford† Alaa Daffalla*
Tara Matthews‡ Sunny Consolvo‡ Jill Palzkill Woelfer§ Patrick Gage Kelley‡
Michelle L. Mazurek† Dana Cuomo¶ Nicola Dell* Thomas Ristenpart*

*Cornell Tech †University of Maryland ‡Google §JumpCloud ¶Lafayette College

Abstract—**Research involving at-risk users—that is, users who are more likely to experience a digital attack or to be disproportionately affected when harm from such an attack occurs—can pose significant safety challenges to both users and researchers. Nevertheless, pursuing research in computer security & privacy (S&P) is crucial to understanding how to meet the digital-safety needs of at-risk users and to design safer**

In this paper, we systematize knowledge from the S&P and HCI research communities to develop pragmatic guidance about reducing risk of harm in the planning, execution, and sharing of digital-safety research involving at-risk users (i.e., *at-risk research* hereafter). Our guidance reflects a systemization of "good" practices based on an analysis of 196 academic works and oral histories from an expert panel

Some examples of at-risk groups

“We define a user(s) as being at-risk if they face an elevated likelihood of an attack to their digital safety, have factors that influence or exacerbate their chances of being targeted, and/or experience heightened harm as a result of a digitally-mediated attack”

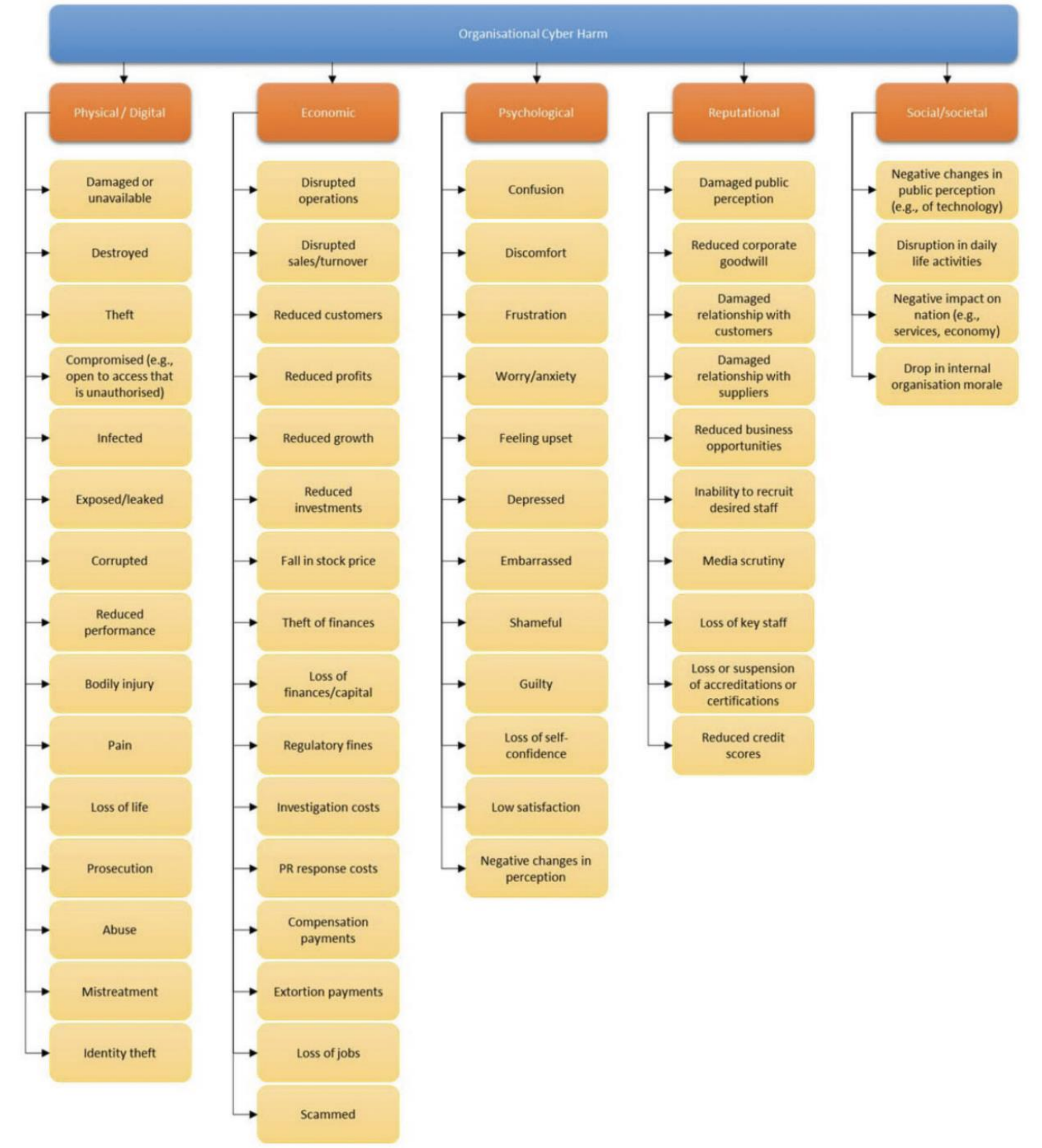
- Survivors of intimate partner violence
- Political activist
- Identity based marginalization (e.g., queer, women, people of color….)

Research questions

- What digital-safety risks are associated with research involving at-risk users?
- What practices do researchers report employing to help mitigate digital-safety risk in at-risk research?
- What pragmatic guidance might researchers follow to reduce the risk of harm in their digital-safety research involving at-risk users?

Method

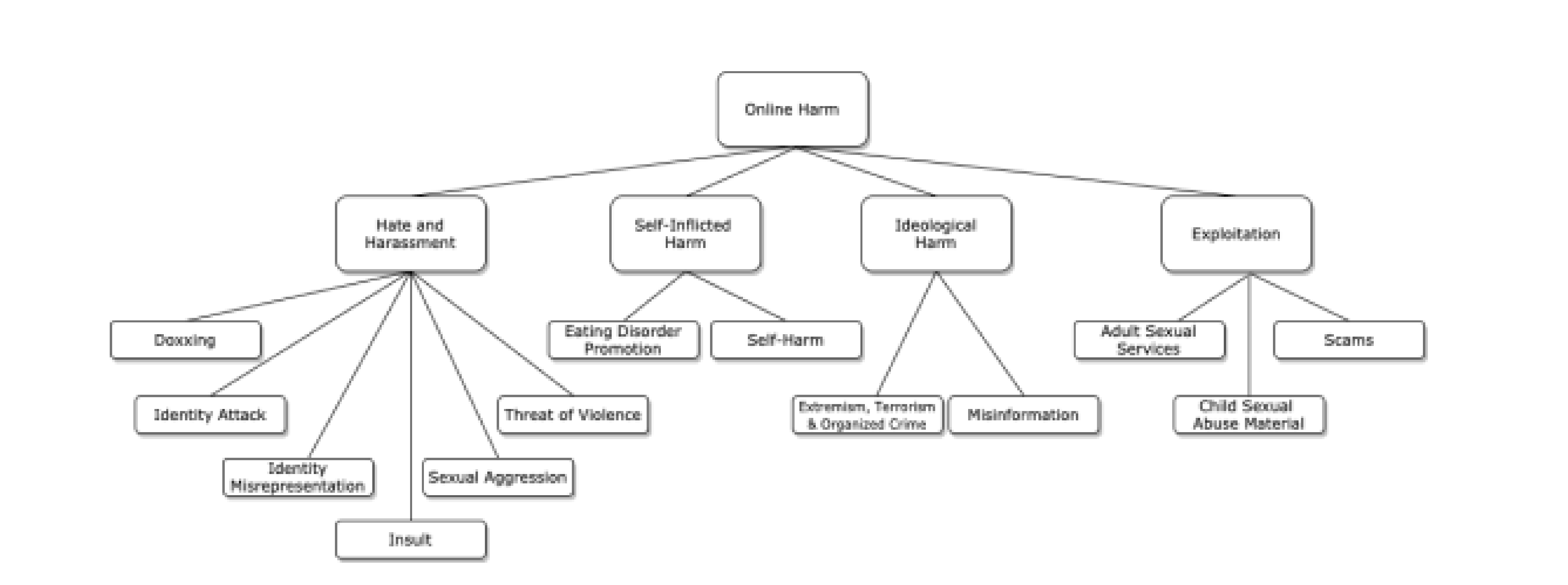
- Materials: 196 peer-reviewed papers in premier S&P and HCI venues after this initial dataset was collected - CCS, CHI, CSCW, IEEE S&P, NDSS, PETS, SOUPS, and USENIX Security
- Approach: qualitative coding and analysis



Organisational Cyber Harm

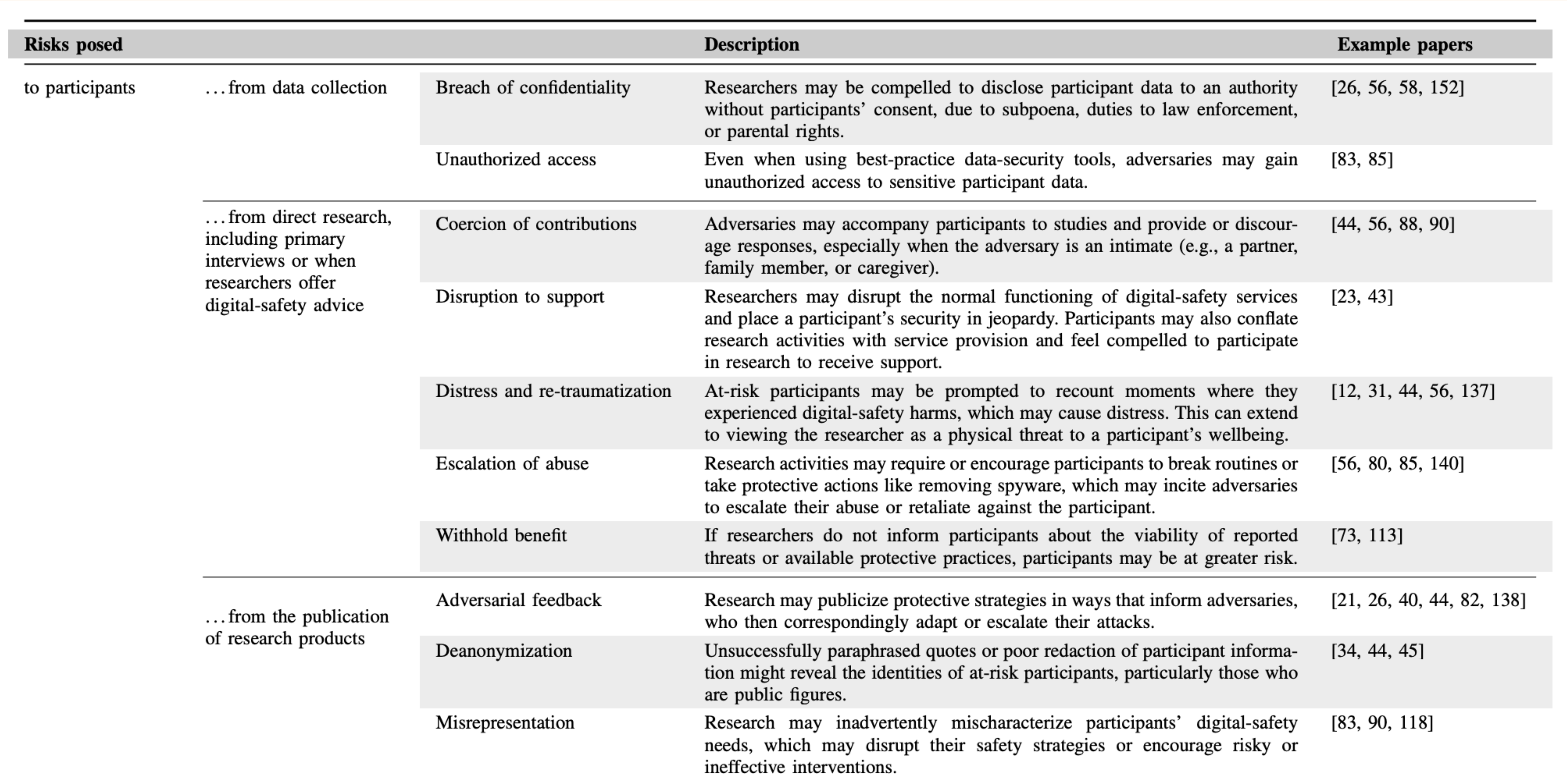
- Physical / Digital
  - Damaged or unavailable
  - Destroyed
  - Theft
  - Compromised (e.g., open to access that is unauthorised)
  - Infected
  - Exposed/leaked
  - Corrupted
  - Reduced performance
  - Bodily injury
  - Pain
  - Loss of life
  - Prosecution
  - Abuse
  - Mistreatment
  - Identity theft
- Economic
  - Disrupted operations
  - Disrupted sales/turnover
  - Reduced customers
  - Reduced profits
  - Reduced growth
  - Reduced investments
  - Fall in stock price
  - Theft of finances
  - Loss of finances/capital
  - Regulatory fines
  - Investigation costs
  - PR response costs
  - Compensation payments
  - Extortion payments
  - Loss of jobs
  - Scammed
- Psychological
  - Confusion
  - Discomfort
  - Frustration
  - Worry/anxiety
  - Feeling upset
  - Depressed
  - Embarrassed
  - Shameful
  - Guilty
  - Loss of self-confidence
  - Low satisfaction
  - Negative changes in perception
- Reputational
  - Damaged public perception
  - Reduced corporate goodwill
  - Damaged relationship with customers
  - Damaged relationship with suppliers
  - Reduced business opportunities
  - Inability to recruit desired staff
  - Media scrutiny
  - Loss of key staff
  - Loss or suspension of accreditations or certifications
  - Reduced credit scores
- Social/societal
  - Negative changes in public perception (e.g., of technology)
  - Disruption in daily life activities
  - Negative impact on nation (e.g., services, economy)
  - Drop in internal organisation morale

Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D., 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), p.tyy006.

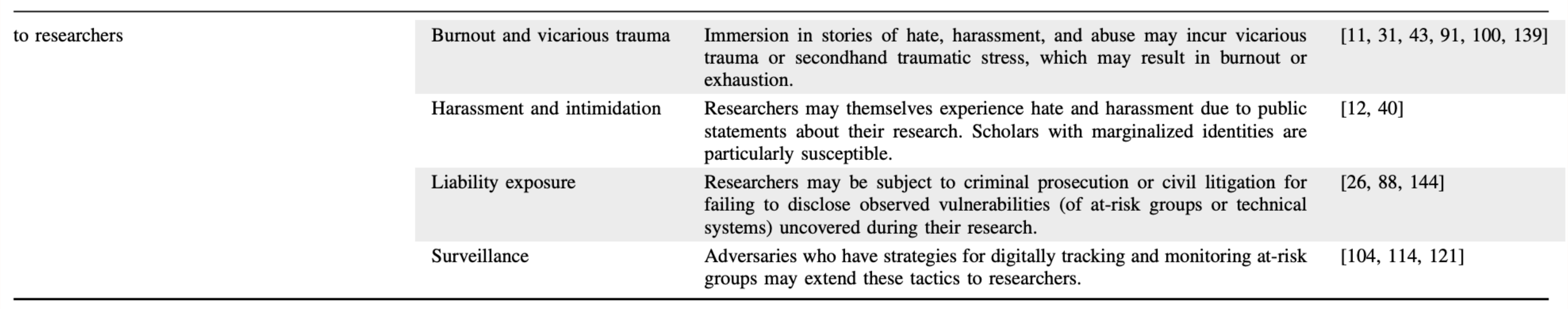


A Unified Taxonomy of Harmful Content

What are the risks in research?



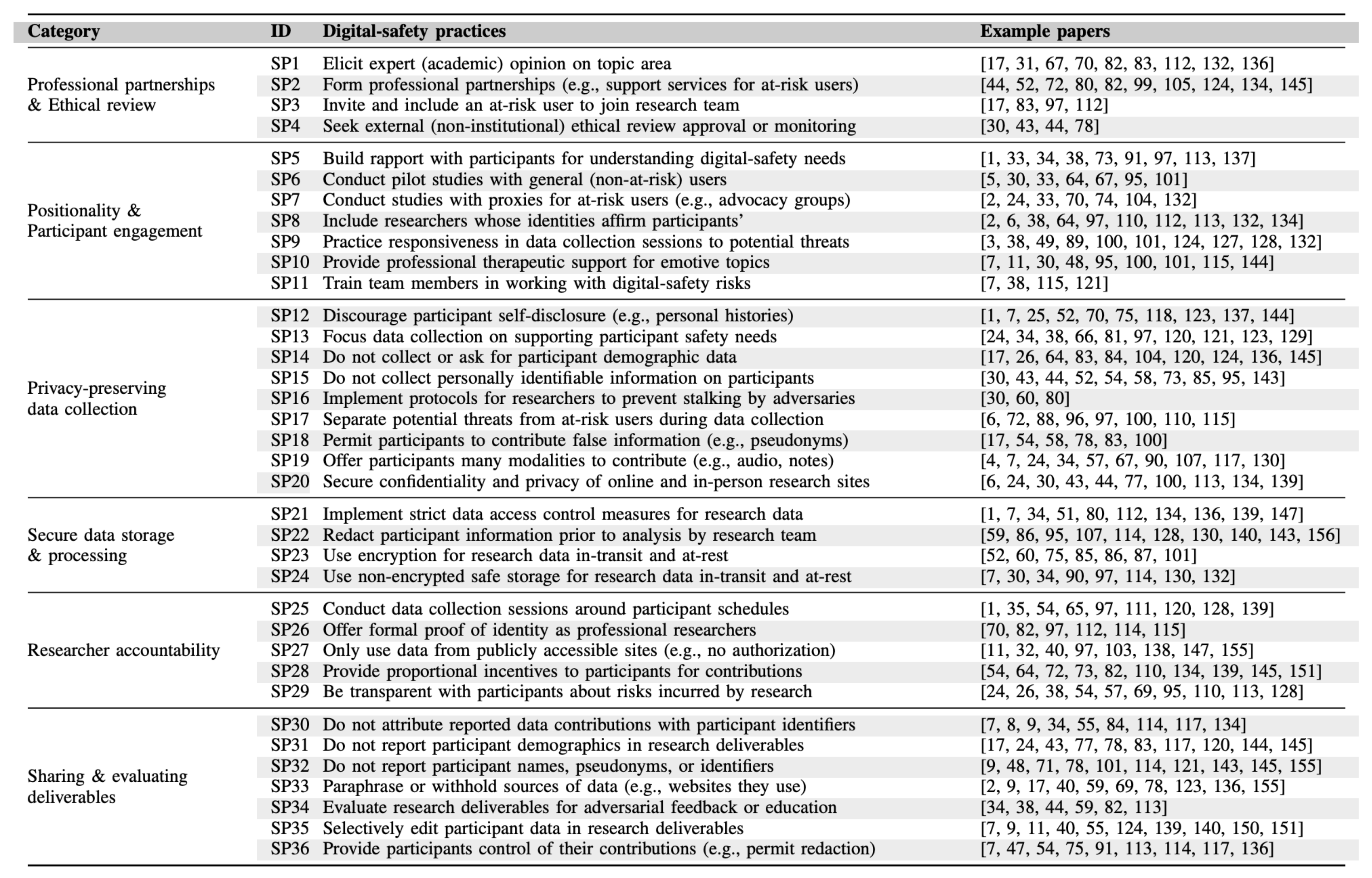
Risks posed			Description	Example papers
to participants	. . . from data collection	Breach of confidentiality	Researchers may be compelled to disclose participant data to an authority without participants' consent, due to subpoena, duties to law enforcement, or parental rights.	[26, 56, 58, 152]
		Unauthorized access	Even when using best-practice data-security tools, adversaries may gain unauthorized access to sensitive participant data.	[83, 85]
	. . . from direct research, including primary interviews or when researchers offer digital-safety advice	Coercion of contributions	Adversaries may accompany participants to studies and provide or discourage responses, especially when the adversary is an intimate (e.g., a partner, family member, or caregiver).	[44, 56, 88, 90]
		Disruption to support	Researchers may disrupt the normal functioning of digital-safety services and place a participant's security in jeopardy. Participants may also conflate research activities with service provision and feel compelled to participate in research to receive support.	[23, 43]
		Distress and re-traumatization	At-risk participants may be prompted to recount moments where they experienced digital-safety harms, which may cause distress. This can extend to viewing the researcher as a physical threat to a participant's wellbeing.	[12, 31, 44, 56, 137]
		Escalation of abuse	Research activities may require or encourage participants to break routines or take protective actions like removing spyware, which may incite adversaries to escalate their abuse or retaliate against the participant.	[56, 80, 85, 140]
		Withhold benefit	If researchers do not inform participants about the viability of reported threats or available protective practices, participants may be at greater risk.	[73, 113]
	. . . from the publication of research products	Adversarial feedback	Research may publicize protective strategies in ways that inform adversaries, who then correspondingly adapt or escalate their attacks.	[21, 26, 40, 44, 82, 138]
		Deanonymization	Unsuccessfully paraphrased quotes or poor redaction of participant information might reveal the identities of at-risk participants, particularly those who are public figures.	[34, 44, 45]
		Misrepresentation	Research may inadvertently mischaracterize participants' digital-safety needs, which may disrupt their safety strategies or encourage risky or ineffective interventions.	[83, 90, 118]



to researchers	Burnout and vicarious trauma	Immersion in stories of hate, harassment, and abuse may incur vicarious trauma or secondhand traumatic stress, which may result in burnout or exhaustion.	[11, 31, 43, 91, 100, 139]
	Harassment and intimidation	Researchers may themselves experience hate and harassment due to public statements about their research. Scholars with marginalized identities are particularly susceptible.	[12, 40]
	Liability exposure	Researchers may be subject to criminal prosecution or civil litigation for failing to disclose observed vulnerabilities (of at-risk groups or technical systems) uncovered during their research.	[26, 88, 144]
	Surveillance	Adversaries who have strategies for digitally tracking and monitoring at-risk groups may extend these tactics to researchers.	[104, 114, 121]

What are the practices?

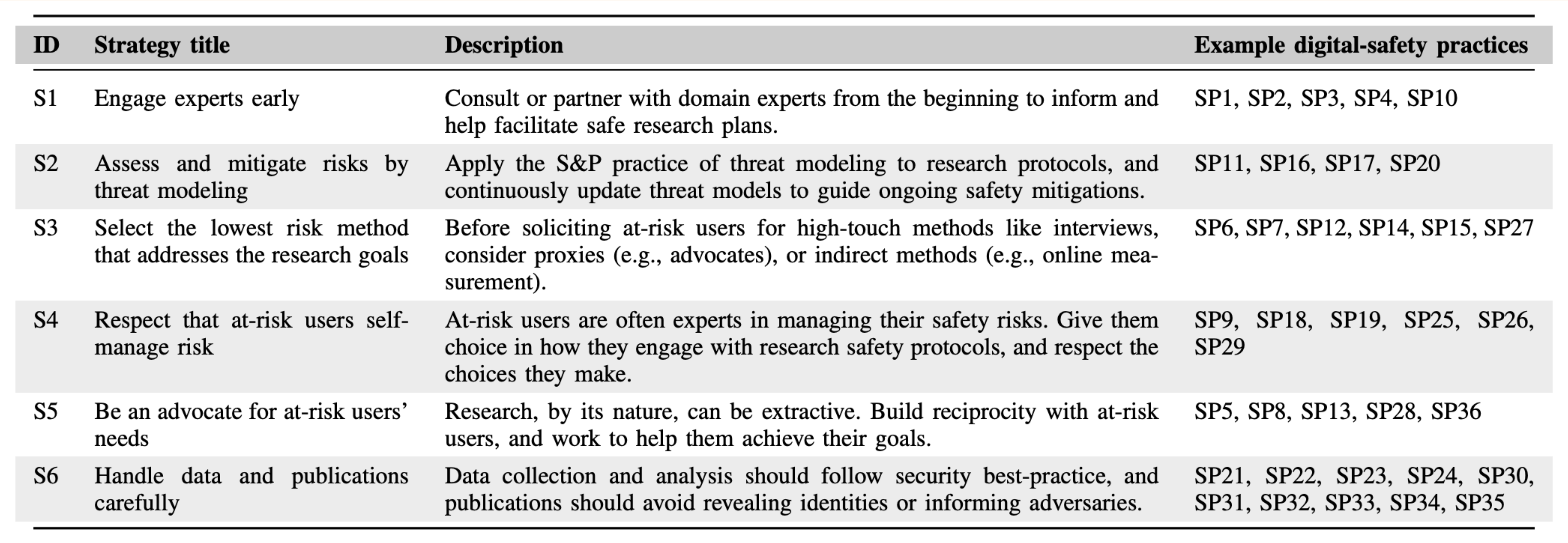
What are the practices?



Category	ID	Digital-safety practices	Example papers
Professional partnerships & Ethical review	SP1	Elicit expert (academic) opinion on topic area	[17, 31, 67, 70, 82, 83, 112, 132, 136]
	SP2	Form professional partnerships (e.g., support services for at-risk users)	[44, 52, 72, 80, 82, 99, 105, 124, 134, 145]
	SP3	Invite and include an at-risk user to join research team	[17, 83, 97, 112]
	SP4	Seek external (non-institutional) ethical review approval or monitoring	[30, 43, 44, 78]
Positionality & Participant engagement	SP5	Build rapport with participants for understanding digital-safety needs	[1, 33, 34, 38, 73, 91, 97, 113, 137]
	SP6	Conduct pilot studies with general (non-at-risk) users	[5, 30, 33, 64, 67, 95, 101]
	SP7	Conduct studies with proxies for at-risk users (e.g., advocacy groups)	[2, 24, 33, 70, 74, 104, 132]
	SP8	Include researchers whose identities affirm participants'	[2, 6, 38, 64, 97, 110, 112, 113, 132, 134]
	SP9	Practice responsiveness in data collection sessions to potential threats	[3, 38, 49, 89, 100, 101, 124, 127, 128, 132]
	SP10	Provide professional therapeutic support for emotive topics	[7, 11, 30, 48, 95, 100, 101, 115, 144]
	SP11	Train team members in working with digital-safety risks	[7, 38, 115, 121]
Privacy-preserving data collection	SP12	Discourage participant self-disclosure (e.g., personal histories)	[1, 7, 25, 52, 70, 75, 118, 123, 137, 144]
	SP13	Focus data collection on supporting participant safety needs	[24, 34, 38, 66, 81, 97, 120, 121, 123, 129]
	SP14	Do not collect or ask for participant demographic data	[17, 26, 64, 83, 84, 104, 120, 124, 136, 145]
	SP15	Do not collect personally identifiable information on participants	[30, 43, 44, 52, 54, 58, 73, 85, 95, 143]
	SP16	Implement protocols for researchers to prevent stalking by adversaries	[30, 60, 80]
	SP17	Separate potential threats from at-risk users during data collection	[6, 72, 88, 96, 97, 100, 110, 115]
	SP18	Permit participants to contribute false information (e.g., pseudonyms)	[17, 54, 58, 78, 83, 100]
	SP19	Offer participants many modalities to contribute (e.g., audio, notes)	[4, 7, 24, 34, 57, 67, 90, 107, 117, 130]
	SP20	Secure confidentiality and privacy of online and in-person research sites	[6, 24, 30, 43, 44, 77, 100, 113, 134, 139]
Secure data storage & processing	SP21	Implement strict data access control measures for research data	[1, 7, 34, 51, 80, 112, 134, 136, 139, 147]
	SP22	Redact participant information prior to analysis by research team	[59, 86, 95, 107, 114, 128, 130, 140, 143, 156]
	SP23	Use encryption for research data in-transit and at-rest	[52, 60, 75, 85, 86, 87, 101]
	SP24	Use non-encrypted safe storage for research data in-transit and at-rest	[7, 30, 34, 90, 97, 114, 130, 132]
Researcher accountability	SP25	Conduct data collection sessions around participant schedules	[1, 35, 54, 65, 97, 111, 120, 128, 139]
	SP26	Offer formal proof of identity as professional researchers	[70, 82, 97, 112, 114, 115]
	SP27	Only use data from publicly accessible sites (e.g., no authorization)	[11, 32, 40, 97, 103, 138, 147, 155]
	SP28	Provide proportional incentives to participants for contributions	[54, 64, 72, 73, 82, 110, 134, 139, 145, 151]
	SP29	Be transparent with participants about risks incurred by research	[24, 26, 38, 54, 57, 69, 95, 110, 113, 128]
Sharing & evaluating deliverables	SP30	Do not attribute reported data contributions with participant identifiers	[7, 8, 9, 34, 55, 84, 114, 117, 134]
	SP31	Do not report participant demographics in research deliverables	[17, 24, 43, 77, 78, 83, 117, 120, 144, 145]
	SP32	Do not report participant names, pseudonyms, or identifiers	[9, 48, 71, 78, 101, 114, 121, 143, 145, 155]
	SP33	Paraphrase or withhold sources of data (e.g., websites they use)	[2, 9, 17, 40, 59, 69, 78, 123, 136, 155]
	SP34	Evaluate research deliverables for adversarial feedback or education	[34, 38, 44, 59, 82, 113]
	SP35	Selectively edit participant data in research deliverables	[7, 9, 11, 40, 55, 124, 139, 140, 150, 151]
	SP36	Provide participants control of their contributions (e.g., permit redaction)	[7, 47, 54, 75, 91, 113, 114, 117, 136]

Better practices?

Safer practices



ID	Strategy title	Description	Example digital-safety practices
S1	Engage experts early	Consult or partner with domain experts from the beginning to inform and help facilitate safe research plans.	SP1, SP2, SP3, SP4, SP10
S2	Assess and mitigate risks by threat modeling	Apply the S&P practice of threat modeling to research protocols, and continuously update threat models to guide ongoing safety mitigations.	SP11, SP16, SP17, SP20
S3	Select the lowest risk method that addresses the research goals	Before soliciting at-risk users for high-touch methods like interviews, consider proxies (e.g., advocates), or indirect methods (e.g., online measurement).	SP6, SP7, SP12, SP14, SP15, SP27
S4	Respect that at-risk users self-manage risk	At-risk users are often experts in managing their safety risks. Give them choice in how they engage with research safety protocols, and respect the choices they make.	SP9, SP18, SP19, SP25, SP26, SP29
S5	Be an advocate for at-risk users' needs	Research, by its nature, can be extractive. Build reciprocity with at-risk users, and work to help them achieve their goals.	SP5, SP8, SP13, SP28, SP36
S6	Handle data and publications carefully	Data collection and analysis should follow security best-practice, and publications should avoid revealing identities or informing adversaries.	SP21, SP22, SP23, SP24, SP30, SP31, SP32, SP33, SP34, SP35