

Surveillance in the Name of Security: A Tension at the Heart of SOUPS?

Gabriel Grill^{1,2}

¹Interdisciplinary Transformation University Austria (IT:U), Linz, Austria

²TU Delft, Delft, Netherlands

The case of risks analytics highlights how security can motivate the expansion of surveillance, contradicting SOUPS's privacy aims, and how individualized privacy falls short when collective actions, like protests, are targeted. The paper problematizes the build-up of security/surveillance and privacy technologies that stabilize each other instead of addressing underlying social concerns and provides recommendations for researchers.

I. THE CASE OF RISK ANALYTICS

In this position paper, I aim to draw attention to a tension, arguably, at the center of SOUPS, namely, how (cyber)security is used to justify intrusive surveillance and thereby can undermine the symposium's aims to advance privacy. In previous work [1]–[4], I have examined risk analytics systems that promise to shield companies from internal and external threats by marking individuals and/or collectives as risky. These blurry and broad categories can encompass a disgruntled employee who may attack crucial systems and, similarly, peaceful protest and labor organizing within a company or across supply chains [2], [3].

When such systems focus on unrest or protest as a category, they center collectives, highlighting limits of individualized notions of privacy popular within privacy scholarship [5], [6] that focus on personal information and technological approaches like differential privacy or aggregation. Such systems can analyze data collected in the workplace [7], [8] or information available on the internet such as social media data [2]. My work illustrated how such analytics efforts are based on controversial, faulty science, like emotion recognition [3], [9], [10], which tends to yield false positives, reproduces problematic societal biases, and creates chilling effects as certain forms of language become risky. When these tools correctly identify activity, they may undermine legitimate forms of democratic and workplace participation, like protests and labor organizing. For example, labor strike prediction via sentiment analysis may be used to enact preemptive measures early on, and network analysis methods could be used to identify influential individuals, which then can become targets.

Considering the devastating consequences a security breach or an act of violence can have, it is reasonable and often also a legal requirement [8] to have appropriate risk management in place to mitigate harms. However, the prevalence of ideologies such as technological solutionism [11], [12] and securitization [13] tend to produce a drive toward evermore surveillance to acquire huge amounts of data for automated analysis and AI products. It motivates the build up of invasive risk profiling

infrastructures that encourage watching from afar and produce suspicion [14] instead of enabling open communication, addressing underlying structural and social problems, and a culture of listening to concerns. The implementation of risk mitigation involves political decisions about power and accountability, and can not be reduced to mere technical matters.

II. USABLE TO WHOM?

One laudable goal of SOUPS is to make security and privacy more usable and widely accessible; however, framing them as usability concerns deprives them of their socio-political character, which risks depolitization and promoting technosolutionism. The build-up of digital surveillance as part of securitization rests on imperial and military roots [15] and a desire to increase the ease and speed of control that manifests in usable technologies such as expansive dashboards and AI products. This rise in surveillance results in public concerns and, thus, motivates work under the banner of privacy. However, privacy can be an ally to surveillance [5] when it is defined as an individual matter and narrowly formalized, e.g., in (usable) technologies or laws. It can then act as a foil that leaves the build-up of surveillance infrastructure unchallenged as, for example, aggregation can be presented as a remedy. The result is a productive loop where both privacy and security/surveillance technologies stabilize each other and are expanded together.

This loop points to a possible conflict of interest within communities, like SOUPS, which envision and build usable technologies for security and privacy. This may also be reflected in the sponsorship of large technology companies, which create surveillance technologies; however, also build corresponding privacy technologies, which may curb public grievances and appear compliant while not addressing the underlying political questions. Thus, challenging the expansion of surveillance requires recognizing that security, privacy, and usability are political categories and their definition and operationalization are part of political struggles. For example, usability can stand for seamless design when efficiency is valued, but friction can also be important as it can offer the pauses needed for reflection and deliberation, making decisions more intentional. I aim with this contribution to encourage reflexivity and debate within the community on tensions regarding privacy, security, and usability, and motivate research that seeks to address them in a way that centers values like worker rights, democracy, and justice.

REFERENCES

- [1] G. Grill, “Researching Online Labor Strike and Protest Prediction Technologies,” in *AoIR Selected Papers of Internet Research*, 2020.
- [2] —, “Future protest made risky: Examining social media based civil unrest prediction research and products,” in *Computer Supported Cooperative Work (CSCW)*. Springer, 2021, pp. 1–29.
- [3] G. Grill and C. Sandvig, “Military AI’s Next Frontier: Your Work Computer,” in *Wired*, 2023. [Online]. Available: <https://www.wired.com/story/military-ais-next-frontier-your-work-computer/>
- [4] G. Grill, “Risky Complaints: Unpacking Recent Trends in Risk Assessment Across Global Supply Chains,” in *EWAF’24: European Workshop on Algorithmic Fairness*, 2024.
- [5] S. Coll, “Power, knowledge, and the subjects of privacy: Understanding privacy as the ally of surveillance,” in *Information, Communication & Society*, vol. 17, no. 10, 2014, pp. 1250–1263.
- [6] A. Marwick, “Privacy Without Power: What Privacy Research Can Learn from Surveillance Studies,” in *Surveillance & Society*, vol. 20, no. 4, 2022, pp. 397–405. [Online]. Available: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/16009>
- [7] W. Christl, “Digitale Überwachung und kontrolle am arbeitsplatz: Von der ausweitung betrieblicher datenerfassung zum algorithmischen management?” p. 152, 2021. [Online]. Available: <https://crackedlabs.org/daten-arbeitsplatz>
- [8] —, “Employees as Risks,” 2024. [Online]. Available: <https://crackedlabs.org/en/data-work/publications/securityriskprofiling>
- [9] G. Grill and N. Andalibi, “Attitudes and Folk Theories of Data Subjects on Transparency and Accuracy in Emotion Recognition,” vol. 6, pp. 78:1–78:35, 2022. [Online]. Available: <https://doi.org/10.1145/3512925>
- [10] G. Grill, “Constructing Certainty in Machine Learning: On the performativity of testing and its hold on the future,” 2022. [Online]. Available: <https://osf.io/zekqv/>
- [11] E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, first edition ed. PublicAffairs, 2013.
- [12] S. Lindtner, S. Bardzell, and J. Bardzell, “Reconstituting the Utopian Vision of Making: HCI After Technosolutionism,” in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’16. Association for Computing Machinery, 2016, pp. 1390–1402. [Online]. Available: <http://doi.org/10.1145/2858036.2858506>
- [13] P. Petit, “‘Everywhere Surveillance’: Global Surveillance Regimes as Techno-Securitization,” in *Science as Culture*, vol. 29, no. 1. Routledge, 2020, pp. 30–56. [Online]. Available: <https://doi.org/10.1080/09505431.2019.1586866>
- [14] G. Grill, “Algorithms as Forward Salients: Examining the Politics of Algorithmic Infrastructure,” 2025, Thesis. [Online]. Available: <https://deepblue.lib.umich.edu/items/acc57560-09e5-41eb-96b1-50bb491a366d>
- [15] M. Wei and M. Fassl, “Towards anti-imperialist security, privacy, and safety research in HCI,” in *Proceedings of the 2025 New Security Paradigms Workshop*, 2025, pp. 37–49.