What is a Privacy Success?

Glencora Borradaile
School of Electrical Engineering and Computer Science, Oregon State University

Perfect privacy, when it comes to digital information, is as good as impossible. Privacy-enhancing technology (PET) development and advances in protecting information systems have improved online privacy and reduced risks to digitized information. Usable privacy researchers and developers have focused on improving the usability and learnability of PETs, as exemplified by the "Why Johnny Can't Encrypt" papers [1], with the implicit idea that use of end-to-end encrypted tools is the ultimate goal. However, even without humans in the loop creating unintentional vulnerabilities as users or developers, there is little hope of a perfectly secure system that would support perfect online privacy. In the absence of perfect systems, though, perfect digital privacy may only be achievable through complete abstention from digital technologies, which is not a practical suggestion in our modern era. Rather than focusing only on better systems, more PETs, improved usability, easier learnability, we should also be asking, **"What is privacy?"** and measure privacy success with respect to that question.

Communications, legal and philosophy scholars have asked this question and put forth definitions of privacy that have evolved as our collective communication practices have changed and as surveillance technologies have grown in capability. The most modern and thorough theory of privacy is Helen Nissenbaum's contextual integrity [2] which, beyond describing the parameters (subject, sender, receiver, data type, means of transmission) that must be identified to fully describe the privacy of an action, emphasizes the need to also identify the *context* in which the information exists as different privacy norms and goals exist in different contexts. Bringing contextual integrity into the world of privacy-enhancing research, we can ask what privacy is sought (or could be sought) by individuals and groups and ask, **"What is a privacy success?"** in that context. Going further, understanding where success is not achieved, again, within the framework of contextual integrity, can help identify where technology is failing to support privacy success and work to develop tools and practices to fill *sought-after* privacy gaps.

My interest in these questions comes from a decade of experience providing digital privacy guidance to social movement groups in the United States. Social movement participants have historically been subject to government and corporate surveillance to degrees that shift with public support and government control [3, 4]. The guidance available to such participants is often lacking, from focusing on the "average" person, to expecting a level of effort that would impact their organizing or encourages a defeatist attitude. The guidance available does not fully account for the context in which privacy is desired. This line of inquiry became focused in a research project, with my collaborators Kretschmer and LeClerc, seeking to understand the factors impacting the privacy of social movement groups' activities during which it became clear that measuring success as use of end-to-end encrypted technologies flattened our understanding of their experiences. We find social movement groups are very aware of surveillance and the risks involved in their activities. But groups make

context-dependent choices on whether to use PETs that go beyond simply deciding whether their information is protected to the highest level.

Even in the era of plug-and-play PETs, and even when those tools are being adopted, we should be asking whether simply adopting those tools is really a privacy success. Consider a few scenarios. Someone uses a VPN as a default practice to protect their privacy from Google and other large internet companies, but they are always logged into their Google account and regularly search for directions on Google Maps from their location. Someone uses Proton for access to end-to-end encrypted email but mainly emails non-Proton email users. Someone uses Signal for a top-secret group chat but adds people not in the need-to-know to the group [5]. In the first example, there is a mismatch of the parameters of the activity with the privacy context. In the second example, mixing transmission protections in the same tool may hide the fact that privacy is not achieved. In the third example, the use of a privacy-enhancing app fails to address misuse of the app, whether it was privacy-enhancing or not. In each of these cases, the information senders are using PETs but not achieving privacy.

To better understand when we can claim a privacy success, I do not propose abandoning use of PETs as a technological measure of success but propose augmenting this measure of success with an orthogonal human measure of whether there is intention around privacy in one's communications and data. In this framing, we can view these human and technological measures as spectrums of success and pair this with the context in which privacy is sought to understand whether success is achieved. In our research on social movement group navigation of technology and surveillance and my experience advising activists on digital privacy, we find examples of each type.

		Technological measure	
		Low use of PETs	High use of PETs
Human measure	Low privacy intention	Human and tech privacy failure	Human privacy failure, tech privacy partial success
	High privacy intention	Human privacy success, tech privacy failure	Human and tech privacy success

We find many groups that intentionally consider privacy when making communications decisions and opt to use PETs as a result. We view this as a privacy success, both from a human and technological viewpoint. (Lower right quadrant of table.)

Many groups make digital communications choices without considering privacy and instead focus on cost or ease of use as a primary deciding factor. As a result, they did not adopt PETs. This is a privacy failure from both a human and technological viewpoint. (Upper left quadrant of table.)

There are a few groups with low privacy intention who do use PETs but do so accidentally. (Upper right quadrant of table.) This use of PETs is not paired with the

operational security protocols necessary to say that privacy is achieved in a meaningful way. While technologists may still count this as a privacy success, I would argue that is unlikely to be a success in the context of humans making day to day decisions on the use of that technology, as argued in our scenarios above.

Finally, and perhaps most interesting, are those groups with high intentions regarding privacy who still opt to not use PETs. (Lower left quadrant of table.) The reasons for this vary. In some cases, groups opt to communicate in person (forgoing digital communication altogether) and in some cases opt for less private platforms to appear more like the rest of society. In either case, this is a failure of technology to produce something trustworthy enough both from a technological soundness perspective and a social norms perspective. These challenges have existed for a long time. Gaw, Felten and Fernandez-Kelly examined the social context behind user's decisions to use end-to-end encrypted email (in 2006, when such adoption was non-trivial) and found that using such a non-standard communication protocol could signal paranoia and lead to underuse [6].

Placing this lower left quadrant of these two measures within the framework of contextual integrity, I would nevertheless classify these cases as a human privacy success as privacy intentions are in essence changing the context of communications. Of course, even those social movement groups who are using PETs intentionally are rarely using PETs for all their digital communication needs. They are often making choices to use PETs for some communications and mainstream, public, or less-private technologies for other communications, depending on the *context* of their needs. That is, context can be considered at any scale, from very large-scope domains used to motivate contextual integrity, such as financial and educational, to very locally defined domains such as external communications versus internal communications of a social movement group.

We can now use this three-dimensional measure of privacy success – along axes of privacy intention, PET adoption and context, to help frame whether a given instance of communication is a privacy success or failure. This allows a greater refinement on whether we have privacy successes or failures and to further inquire as to how privacy failures can be remedied, whether through education, policy or new technologies.

Acknowledgements Kelsy Kretschmer, Alex LeClerc and NSF Grant No. 1915768.

Bibliography

[1] A. Herzberg and H. Leibowitz, "Can Johnny finally encrypt?" in *STAST* 2016.
[2] H. Nissenbaum, *Privacy in Context*. Stanford University Press, 2009.
[3] D. Cunningham, *There's Something Happening Here*, UC Press, 2004.
[4] S. Zuboff, "Big other" *J. Inf. Technol.*, 2015.
[6] "United States government group chat leaks," *Wikipedia*. May 07, 2025.
[7] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in SIGCHI, 2006.