Feature Guide for High-Risk Contexts (2025)

Superbloom's list of the security and privacy features that people actually want

Background

This feature guide is designed to help designers and developers adapt tools for people whose technology use puts them at heightened risk.

Who is "at heightened risk"? One answer is: we all are, at some point. Digital platforms constantly collect and sell personal data, generally without users really knowing how or when. Nobody is immune to the long-term consequences of massive data exploitation. As Shoshana Zuboff writes in *The Age of Surveillance Capitalism*, "we are the objects from which raw materials are extracted and expropriated for... prediction factories."[1] The level of pushback on this process varies widely by jurisdiction. In the EU, the GDPR aims to curb surveillance power and strengthen individual digital rights by enforcing strict data protection laws and, at least theoretically, holding companies accountable for misuse. But much of the world lacks these regulatory frameworks. Personal data is often freely harvested and exploited by both state and corporate entities, with little oversight or recourse. Therefore, as market pressures push towards profit at the cost of individual interests, and in the absence of strong regulation, our exposure to risk shifts unpredictably. By this logic, as long as these forces continue unchecked, every user is at heightened risk.

But while we all face risks, we don't all face them equally. Consider that a woman of color posting selfies on social media is statistically more likely to experience harassment than a cis white man doing the same. A group chat organizing an anti-government protest in Serbia puts participants at higher risk than if the same group of people were organizing a games night. Some tech users are more likely than others to experience adverse consequences, based on

[1] Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

where they are located, who they are, or what they are doing. In our work, we often encounter people working in “high-risk” technology use contexts:

- People who work or participate in activities (human rights, advocacy, activism, journalism, support, etc) in an environment where that **work is criminalized, culturally or socially stigmatized**, or otherwise puts them at risk of surveillance, scrutiny, or harm by state actors or interpersonal contacts.
- People whose **access to the internet is restricted or cut off** through censorship or shutdowns, causing them to rely upon circumvention technologies to access the open internet.
- People who **belong to a marginalized social group** (e.g. a religious minority, LGBTQIA2S+, etc) in their region, country, or community and are victimized by virtue of their identity with or affinity to those groups.
- People whose ability to **exercise their human and civil rights is affected** by group or political affiliation.
- People for whom **security and/or safety is a primary factor** in their decisions about what tools to use, how they work, and how they communicate. Security is a necessity, not a nice-to-have.

A 2025 article by Tang et al. proposes a layered model of vulnerability, placing the individual at the center.[2] An individual’s vulnerability may be influenced by factors like race, gender, sexuality, income, and health. But these demographic factors alone do not paint the full picture of a high-risk situation. As the above list illustrates, vulnerability arises through interactions between the individual and their context – factors as diverse as governments, ideologies, family ties, employers, births, deaths, and natural disasters can cause shifts in how risky a certain behavior is. This model highlights why designing for "high-risk users" based on their demographics doesn’t match up with real life. Risk is dynamic, influenced by multiple external layers, and can shift rapidly in response to changing circumstances.

[2] Tang, Xinru, Gabriel Lima, Li Jiang, Lucy Simko, and Yixin Xou. 2025. Beyond “Vulnerable Populations”: A Unified Understanding of Vulnerability from a Socio-Ecological Perspective. *Proceedings of the ACM on Human-Computer Interaction* 1 (1): 0–30. https://yixinzou.github.io/publications/pdf/cscw2025-tang-preprint.pdf.

Our high-risk design philosophy

In an ideal world, all tech tools would be resilient enough for high-risk contexts, and the top tier of security and privacy would be attractive and usable enough for everyone. But this just isn't realistic. For a variety of reasons, many tools that offer more security and privacy are not always an optimal choice for people who are less concerned about safety, and certain precautions have convenience tradeoffs.

However, it's also not realistic to expect that people in high-risk contexts will prioritize only security and privacy and therefore adopt a completely different set of tech tools. In our research over the years, we have found that people weigh security and privacy along with network effects, availability, ease of installation, ease of use, and a host of other factors.

Therefore, this list of features advances a UX design philosophy that smooths the bump between "high-risk context" tools and "everyday" tools. We aim to create some helpful overlap between these categories. Though these categories will never merge entirely, we hope they grow closer.

To make this philosophy a reality, our feature list follows the following principles:

- **Refine specialized equipment, but also strengthen everyday tools.** There will always be a role for both types of apps and services. If a tool ends up straddling this boundary, so much the better.
- **Ensure technology doesn't obstruct users' existing ability to navigate high-risk situations.** Sometimes, the best design choice is to get out of the way and let people continue to use their own social processes.
- **Provide features that reduce vulnerabilities without being intrusive.** For example, offering easy-to-use privacy settings and pseudonymity options can give people choices without making too many choices for them.
- **Acknowledge and incorporate real-world usage patterns.** If technologists learn about people creatively using their technology in order to reduce risk, they can refine features accordingly.

Some teams design highly specialized technology that really only makes sense in high-risk contexts. If this describes you, your tool will almost certainly benefit from including many of these features.

Other teams create adaptable, resilient technology that can flex along with different levels of risk. If this describes you, these features will help your tool adapt to changes in the risk context.

This list is a menu of possibilities. No tool should include all these features – that wouldn't make sense. Some of the features even conflict with each other. However, given the types of use cases that seem most likely for the tool being created, some of these features may stand out to you as an easy win, straightforward to implement, or something people would likely really appreciate.

By recognizing the multifaceted, contextual nature of risk and designing with flexibility and adaptability in mind, we can create tools that mirror and support the resilience of the people using them.

A permanent work in progress

This is a compilation of safety and security-related features that we have noticed people bring up in our research projects since 2018. We further developed the list through a 2024 workshop we hosted with other designers and tool builders in the space.

This type of list is, by necessity, a work in progress. We hope to expand and revisit this list yearly. Technologies and user habits change, and so do the digital threats people face.

If you see something we are missing, please let us know. Even better, if you would like to take part in a mini-workshop to update the list, reach out to us! We find that group settings work particularly well for exchanging this type of information. Write to us at hi@superbloom.design.

Thank you to workshop participants Chido Musodza (Localization Lab), Phirany (Ok Thanks), Ella (Okthanks), and Holmes Wilson (Quiet) for their contributions to this list. Thank you, as well, to all interviewees in high-risk contexts for sharing your do's and don'ts, your wish lists, and your wisdom.

Feature List

These features fall into five broad categories.

1. **Features that disguise** help people hide their use of the tool.
2. **Features that delete** help people easily make their data go away.
3. **Features that educate** give people hints and reminders relevant to privacy and security.
4. **Features that welcome** make your tool pleasant and straightforward to use.
5. **Features that support social dynamics** let people use the group structures and roles that work best for them.

Features that disguise

How they help

Disguise features hide the fact that somebody is using a particular app. This makes it less likely that somebody looking at the device – either by seizing and searching the device in an official capacity, or just sneaking a look at the screen – will see that the app is on the device and being used.

Limitations

These features do not actually remove data from the device. They protect against a casual physical search.

Feature	What it is	Pros, Cons, and Notes
App disguise	Users can disappear or disguise an app from a phone homescreen (e.g. the app icon becomes a calculator, a weather app, a stock app, or similar).	*Pros:* ➕ Helps to obscure activity. ➕ In the case of seizure, people may not think to look through e.g. a calculator. *Cons:* ➖ Does not protect in the case of any kind of forensic analysis on the device or a more thorough search. *Notes:* ● Many of the most savvy mobile users in this risk group will take proactive steps

Feature	What it is	Pros, Cons, and Notes
		on their own to achieve app invisibility: they will uninstall apps, clean devices, or use alternative devices or alternate identities on devices when at risk of device seizure. • Some users just want a niche enough app that others don't know to look for, rather than a popular app that can be disguised.
Hiding critical information within app	The app is visible, but the user can trigger a mode that locks/hides sensitive information, such as names, phone numbers, and messages. This can either apply to all data, or only to data marked sensitive, so that the user isn't left with a suspiciously blank screen.	*Pros:* ➕ Some users told us that this was even more helpful than being able to hide the app altogether. *Cons:* ➖ Not always useful: for example, in some particularly repressive contexts, the authorities will beat/torture/question the owner of the device until some of this information is uncovered. *Notes:* • Users are concerned about apps and devices looking "suspiciously clean."
Browser version of app available	Users don't have to download an app. They can achieve the same functionality by using a mobile-optimized web app.	*Pros:* ➕ Unless the app can be easily hidden, some users feel it's too risky to install certain apps and perceive browser-based use as having less of a "footprint" on their devices. ➕ This is useful for those who may not have a phone that is compatible with an app or who need a secondary way to communicate if they have security/safety concerns. ➕ If the adversary is large (e.g. nation-state), users want to limit the attack surface. That means only installing browser + VPNs + Signal on devices in some cases. *Notes:* • Some users use browser tabs for managing tasks and organizing apps;

Feature	What it is	Pros, Cons, and Notes
		these users seem to be okay with locally-running apps as long as they can run in browser tabs.
Unobtrusive branding	It's not immediately obvious to a casual observer that the app or service is being used. At a glance, the screens look generic, or even look similar to another common app.	*Pros:* ➕ Useful for the purposes of "hiding the app in plain sight." *Cons:* ➖ Accompanying safety tactics around using such apps are an essential pairing. *Notes:* ● If the logo, colors, and name appear frequently, for example on a splash or loading screen, everyone around the user can tell what app they're using. ● Users expressed that censored or blocked services whose branding is quite loud or obvious makes them feel less safe while using those apps.

Features that delete

How they help

Deletion features make data either disappear, or not be created in the first place. This applies to both data and messages sent intentionally between users, and to data that is automatically generated from a user's use of an app. Minimizing and deleting data makes it more difficult to track or prove use of the app, as well as creating less vulnerability in the case of access or search.

Limitations

In many cases, users have to activate these features – that is, they have to choose to delete the data. If they don't know that this is a good idea in a certain situation, they might not do it.

The traceless deletion features requested in high-risk contexts often come at the cost of transparency. One reason many apps currently do show "This message was deleted" or similar is to lessen confusion and let others follow what happened. One approach might be to give administrators of a community the option to turn traceless deletion on or off.

Vanish mode	Available in Instagram, an interesting twist on disappearing messages: messages go away when vanish mode disabled.	*Pros:* ➕ Users report people forgetting to change disappearing messages, which can create data loss when times are too short or inappropriate retention when times are too long.
Metadata guardrails and alerts	When a piece of media is shared, the metadata is easy to see and/or users get alerts about the metadata attached, so that users know what metadata is being shared along with their photo/video/file.	*Notes:* • Activists and journalists in group chats worry that less digital security literate members may not be aware of the metadata attached to the media they share. • Some users want to have a button that immediately deletes all chat history.
Message deletion with no footprint	When a user deletes a message, the app doesn't show a log of message deletions.	*Pros:* ➕ Perceived as a very important feature particularly for people in the field *Cons:* ➖ Could put people in a difficult situation if there is no record of their communications *Notes:* • Though content is deleted, the evidence that messages were sent between parties can still make people vulnerable to authorities/analysis. • Telegram currently offers this feature. • Example about NYC mayor Eric Adams' deleted Signal messages that didn't actually protect him from the mobile forensics that were investigating who we contacted and when.
Remote deletion of all content upon removal, if possible	Some users and organizations want to be able to remove someone from all groups and ideally delete all messages from the person's device if possible, e.g. in an arrest scenario.	*Notes:* • Some groups preferred Telegram over Signal due to Telegram having more robust and less visually obvious deletion.

Ability to limit what activity history is on the device vs. what is on the server	If authorities put a phone into airplane mode to prevent remote deletion, it is desirable if their access is limited.	*Pros:* ➕ In an emergency, the ability to wipe activity history or leave generic-looking activity history on the device is important. *Notes:* • We spoke to one Telegram group that sets the cache size to its lowest limit, so that no messages are stored locally (the opposite behavior from Signal!)
Face blur for photos and videos	Users can easily blur or obscure faces in photos and videos they share.	*Pros:* ➕ Great for protection of sources. *Cons:* ➖ Needs to be paired with wiping metadata from images and video for more privacy. ➖ Can this provide a false sense of security? Depending on how the blur is executed, it can be reversed. *Notes:* • Activists documenting human rights abuses, police brutality, etc. want this feature seamlessly integrated to their messaging apps
Maximum retention limits	Users want to be able to set maximum retention limits / disappearing messages times as an admin	

Features that educate

How they help

Education features explain to users ways in which they might want to use the tool to enhance their own privacy and security practices.

Limitations

Some users won't read or use these tips. Use them as a supplementary measure to protect users, not the first line of defense.

Sensitive messaging assistance	Enables users to break messages up and send them in different formats – e.g. a story that can be sent in three parts: part 1 as 1-to-1 text, part 2 as voice note, and part 3 as a phone call.	*Notes:* • Privacy-conscious users already take these precautions, so process prompts or help breaking up messages and piecing them back together afterwards would be ideal.
Appropriate advice	Offering or linking to appropriate advice related to a tool's function, but for features that might not technically be part of the tool, e.g. how to hide a folder/location on a device.	*Pros:* ➕ Users mention how information upskilling and knowledge sharing in the community enables them to be safer. If not facilitated in person, users report trusting the advice and suggestions of certain apps/tools made by or affiliated with certain organisations.

Features that welcome

How they help

Welcoming features make an app more friendly and familiar to use. If an app with strong security and/or privacy features also has features that welcome users, people are more likely to use it even in lower-risk contexts.

Features that make it easier to communicate are a key component of apps for high-risk contexts. People are safest when they can "speak their own language" – written, stickered, emojied, and voice-memoed. Signal is a common choice of channel for people who need encrypted messaging. Not coincidentally, Signal also offers stickers, stories, and voice messages – not exactly "security features." They explain, and we agree, that "there is no one global norm for how people talk to each other. People have to be able to use Signal to talk to the folks in their lives in the ways that they want to be heard... And if your friends can't use Signal, neither can you." (The stickers, Signal points out, are also end-to-end encrypted.)

This has several benefits. First, if the tool depends on network effects, the more users there are, the easier it becomes to get new people to use it. Second, when people in lower-risk contexts occasionally use a tool that is also suitable for high-risk contexts, it makes the fact of using the tool less likely to arouse suspicion from onlookers or authorities.

Limitations

These features aren't security or privacy features in the strict sense. However, as we've detailed elsewhere, usability and security are mutually beneficial. Usable tools are more secure tools, and vice versa.

Emojis and stickers	Emojis and stickers serve critical communications and freedom of speech purposes when used to circumvent censorship of certain words or topics by governments or by content moderation and algorithmic filtering.	*Notes:* • There are many examples of this phenomenon. One current instance: activists have adopted the 🍉emoji to stand-in for typed words related to Palestine, which helps dodge the shadowbanning of their content.
Voice memos	Users can send a clip of recorded sound as a message.	*Pros:* ➕ One activist we interviewed emphasized that voice notes are critical for inclusivity in activist work: many mobile phone users in Uganda, for example, have low literacy, and voice notes are a critical access need to ensure they can participate online. ➕ Useful when needing to transmit detailed information in the shortest amount of time (time taken to type vs time taken to record and send) *Notes:* • Activists from Uganda, Lebanon, and Azerbaijan shared that they communicate 50/50 in voice notes vs written text. • Multiple shared that they typically type in English while they record voice messages in their local language. • In Brazil, even professional groups like lawyers will use long voice memos to discuss cases
Dark mode	Users want to have the option of a "dark" UI.	*Notes:* • Not exactly a privacy or security feature, but many users are *so* passionate about

		dark mode that the lack of it is a dealbreaker! ● One technologist we spoke to stated, “Dark mode is the single most important security feature, because it's the one people ask for *all the time*."
Simplified set up procedures for apps	Users want to be able to follow very simple instructions to set up/ run an application	*Pros:* ➕ In crisis situations, tool makers want to avoid users abandoning an app because it looks too complicated to set up or run. Participants saw this happen in real time, especially when there weren’t trainings or preparedness activities before the crisis. *Notes:* ● This has been a barrier for apps with many language versions -- when it's too hard to select your language, people just stop trying ● It can even be difficult for users to locate the app in the app store in the correct language if it is one app version with various language settings available after installation.
Let users know the reasoning behind less-than-optimal UX	Users are more willing to forgive unexpected or confusing app behavior if they know what security or privacy trade-offs the technology is making.	*Notes:* ● For some anti-circumvention apps, blockages and VPN issues alike can hinder the display of multimedia content, which is a huge barrier for information-based services, especially ones trying to get information out over video and audio streams. We found that users were quite tolerant of these issues if they were made aware of the reason behind them. ● Letting users know through alerts and banners that active censorship circumvention may be impacting their experience helps them to both understand and value the service.

Features that support social dynamics

Why they're important

Every communication tool has an implicit model baked into it of how the group of people is structured. For example, many tools are designed with the assumption that one person must be in charge; they express this by having a limit of one "owner" of a group, space, or account. If a group doesn't have one person in charge, they are forced to put someone in charge just for the purposes of using the tool. This then has an impact on the social dynamics of the group.

If you're not part of the group yourself, you likely don't know how groups of users are organized. Therefore, you should build flexibility into the structure of your tools so that the tech adapts to the group, not the other way around. Groups often build social structures and practices for a reason—they've figured out what works for their unique dynamics. A good tool should scaffold and support those mechanisms, reinforcing roles and workflows instead of forcing people to bend to an app's design quirks. These features help a communication tool serve a group's structure, not dictate it.

Multiple admins	Being able to have multiple admin accounts instead of a strict hierarchy based on a single owner.	*Pros:* ➕ Removal of an account can be an emergency scenario, and single admin non-availability creates a crisis in these cases ➕ "The most senior people in our org are not always the most competent or the most available"
Suspend / restore	Being able to suspend users and easily restore them without data loss.	*Pros:* ➕ Admins/users often get ambiguous signs that another user might be compromised. Important to be able to err on the side of fast removal, with low cost. *Notes:* ● Password managers often offer this.
In-app identity verification requests	Users can request verification calls and endorse others as verified.	*Pros:* ➕ This is especially important for users who have to navigate constantly changing phone numbers and user names of their trusted contacts. *Notes:*

		• Could support the ways that people already verify contacts (i.e. through a phone call in a separate thread). • Users are interested in other kinds of identity validation systems added to chat apps as well. • Users have a tension between needing memorable names and wanting protection of membership metadata against an attacker who compromises their space
Status updates	Being able to say "out to lunch" / "on a call" in a team context.	*Pros:* ➕ Example of a group that checks in on each other *very* actively when people go silent. A culture of updates in Slack prevents people from worrying and from false alarms. ➕ Another group puts their time zone in their Signal username to set expectations about when you might get a response.
Group chat administration features	Features similar to those available in tools for lower-risk contexts: poll-style voting, broadcast messages, pinned messages, threaded conversations, improved search, and many more.	*Pros:* ➕ Users shared that better control over group chats and their content would help combat information overwhelm ➕ Prevent information overwhelm, draw attention to important information ➕ Notice inactive members so that an admin can tidy up or even delete the group *Notes:* • Users report needing more work / life separation than Signal or Telegram provides (in those apps, all chats and groups are mixed together) • Users who rely on apps like Signal for work and for personal business lamented that they can't administrate very effectively with colleagues/team members on Signal