Privacy and Security

How private is your data on the XR communication services?

Data on our new services is held in an encrypted partition on a server in Switzerland (which has excellent data protection laws). Should we receive the statutory 24 hours notice of a data access request, we only have to shut down the server to make the disk about as much use to the authorities as a brick.

Having said that, data on a public channel in Mattermost, a public forum on UK Forums, or a shared folder on UK Cloud should be considered public -- if anyone in XR can access it, then you should assume there is a mole in the organisation, who can pass it on to the authorities.

All data on **any** server is accessible to the system administrator of the server. This is why we do not recommend using third party servers for anything in the least bit sensitive. The system administrators of all the XR servers (a handful in total) are all long standing XR members who are trusted by the movement.

Mattermost

The system administrators of the Mattermost server (none of whom are in the UK) ask that you **do not** share sensitive details of illegal activity on Mattermost.

Quote from the XR Global FAQ

> The XR Mattermost is a service in use by hundreds of groups, for team chat, group updates and organising. As the service is shared, we need to make sure no one team or group makes this service any more of a target for our adversaries than it already is. If an adversary (including an insider or federal investigator) knows high-value information is stored on this server, they will focus on ways to reach it, including possible legal interventions. As such, the less sensitive and high-value information that is shared on Mattermost, the better for all of us, and it will keep ticking along just fine.

> But what is meant by 'sensitive information'? Here is a non-exhaustive list of examples:
>
> - Home addresses, personal phone numbers and full names of action coordinators
> - Full names of rebels signing up for an action
> - Credit card and bank details
> - Car license plate numbers of rebels
> - Login details for group social media accounts
> - Leaks from truth tellers
> - Date, time, place and participants of a planned clandestine action
>
> Details such as above are best shared off-platform, on an end-to-end encrypted service like Signal, Wire or Session. For sensitive documents, use the end-to-end-encrypted XR Cryptpad. Use MM for chat and for organising (action planning should be in private teams and/or channels), but when the info gets hot, "I'll Signal you those details". This also ensures that if an adversary manages to get their hands on one account, they don't have all the pieces of the puzzle to sabotage an action, nor pair up individuals with a particular action plan, nor put faces to words with intent to commit crime (etc).
>
> We want to be arrested for what we do, not what we plan to do, least of all for a few ideas we're throwing around.
>
> This best-practice approach is referred to in Operations and Information Security as air-gapping as it puts space between mission-critical information and/or infrastructure. It's a great group and mission-centric habit to get into, and is broadly used in gov agencies, military and corporate sectors. It's a trick they don't want us activists to know and use!

Data in a private channel in Mattermost can only be accessed by members of the channel. Only other members of the channel can add new people, so that is the highest level of privacy available to you.

You may notice that private channels created by the XR UK Hub have *xrukadmin* as a member. This is the login of the Hub on Mattermost, and allows the Hub to add and remove members, rename the channel, etc. This function is there to save you work, so that people can be automatically added to your channels when you invite them to the Hub, and so you can remove people, and rename or delete channels from the Hub easily, without having to repeat your actions in the 3 different services.

The UK system administrators have access to this login, so they could, in theory, see everything you say in the channel. If you have something too private to reveal to the UK system administrators, then create a new private channel in Mattermost, rather than via the Hub. Of

course, you will then be totally responsible for administering that channel, adding new people in, removing people you do not want in it, renaming it (in Mattermost), etc.

Please do not remove xrukadmin from a team or channel that has been created by the Hub without letting the system administrators know right away that you have done so -- if the Hub thinks it can access a team or channel, but it can't, that will cause error messages for your users.

UK Forums

Data in private forums on UK Forums can only be accessed by Forum group members (and the UK Forums administrators). You can check who is in the forum group by accessing the Forum Groups option on the Forums main menu, and finding the relevant group. You can remove people from the group by removing them from your organisation on the Hub (preferred), or in UK Forums (but the Hub may add them back again if you don't remove them there too).

UK Cloud

Data in private group folders in UK Cloud can be accessed by group members (and the UK Cloud administrators), and by anyone you share it with. Again, you can remove people from your organisation (and therefore access to your group) on the Hub.

Why are there private working groups?

This is quoted from a post by the global security expert (with minor formatting edits).

Something that comes up often is "Why are there private working groups? Why can't we all work in the open?" My own experiences in several large online communities, is that having private areas facilitates thriving, safer communities. A 'regime of openness', on the other hand, tends to seed decay, even paranoia and distrust. While that may seem counter-intuitive, there are a great many reasons why this is so:

Privacy is not Secrecy

First of all, we need to challenge the misbelief that Privacy and Secrecy are one and the same.

They are not. To quote a beautiful work of literature, *A Cypherpunk's Manifesto* (EN), 1993

"Privacy is the power to selectively reveal oneself to the world."

There are things we would tell a sibling we would not a parent; that we would tell a friend that we would not tell a relative or boss. Privacy is the *glue* of a happy and healthy society, it is how we establish and manage our socio-emotional and physical boundaries.

If I walk up to a couple in the park and demand a summary of what they just talked about, to be included in their conversation, and they refuse, we wouldn't say they are being 'secretive'. Rather,

they are asserting their basic human right to privacy.

So it follows that we should certainly not distrust those that seek and affirm privacy, rather those that rally against it, those that *demand* openness. Further, it should be no surprise that those suspicious of allowances for privacy are often from privileged socio-economic backgrounds.

It must be up to individuals when they choose to be open. This is only something that a *de facto* of privacy, alongside a basic right to anonymity, can provide.

Whole community poisoning

Private working groups also protect against a very real threat to online communities: **Whole community poisoning**. Should a troll or infiltrator, or organised group of such, come to Mattermost or Forums and be able to openly join every one of the dozens of teams on this server, every one of the channels and working groups, they can quickly ruin the social and cultural domains this server affords. Having private working groups and/or areas affords us Circles of Trust:

Circles of trust

Allowing members of private channels to manage those same domains encourages a sense of ownership, of trust. In essence, it embodies a *decentralisation of trust*, in that it is not centrally managed by a vetting process (like a Police file) but rather by transient (a table at a bar) or permanent (a village) communities themselves, through their own experiences (and ever branching degrees of separation).

Like all animals, we meet people, get to know them, and let them closer.

We need to talk about Google Docs

From the XR Global security expert again (slightly edited to refer to XR UK comm's services):

"**Green and Black Cross**, seasoned professionals in the support of activists in need in the UK, made a public statement in 2019 that they would no longer support XR UK. In their statement, one difficult to read, they specifically cite the use of Google (alongside WhatsApp and Facebook messenger) as a risk to rebels, opening them up for deep exposure to Police. Although things have moved on, their statements help to explain why we should not be using Google Docs, WhatsApp, or any other commercial data storage or communication tool for rebel's personal information.

> We believe that the way XR stores personal data is inadequately secure (for example, in Google documents and forms). This means that personal data belonging to LOs is likely to be accessed by police.

> We believe that the communication channels XR uses for legal observers are inadequately secure (for example, WhatsApp and Facebook messenger groups, public Facebook events and email lists with no bcc). This also means that communication through these channels is likely to be accessed by police.
>
> Green and Black Cross, 2019

Their statement raises an old issue here on Organise.Earth [Ed: The server hosting the global Mattermost], one that is a primary motivation for the server existing in the first place: *we endanger each other, and ourselves, when we work with surveillance capitalists*. So let us stop doing it.

Google is a completely unsafe partner for civil disobedience, activism in general. We can't have a 'regenerative culture' and partner with that corporation. *Green and Black Cross* are veterans in this space, and we ought to heed their concerns. I share their concerns having assisted at-risk individuals and groups for years with their infrastructure, to keep them off-police-record and safe in their work.

Lists of Rebels in a Google Doc - any list of contacts - threatens those in less privileged operational environments, where police request information from Google, which they openly provide, to incarcerate that/those individual(s). It would be great to see us take this to heart and understand that it is uncaring and mutually harmful to continue to use Google products, not to mention WhatsApp (a meta-data harvest), as **Green and Black Cross** make so clear.

While an XR NL or XR SE (for instance) may find it unusual/paranoid/specious to have such concern, it is a 'projection of privilege' to assume the same jurisdictional/legal environment exists for all, where brave rebels working in difficult conditions are first surveilled (by statecraft, federal police) and then they are jailed, beaten and/or shot. Many of our rebels work in such environments. In the spirit of regeneration and mutual support, **it is time for our ethics to be reflected in our communication infrastructure**."

Solutions

Use Nextcloud to store and view documents on UK Cloud. Or the XR Global Cryptpad.

Both the Cloud and Cryptpad allow shared editing of documents, but do not expect this to be as slick as Google Docs, which has all the massive resources of Google behind it, and has probably cost millions to develop! Remember that the cost of using Google is that everything becomes easily available to both commercial and state interests.

When someone posts a link to a Google Doc, gently remind them that use of Google is provably unsafe, that we need to make the effort to copy its contents out to a document in our XR owned cloud. It is not just the content of the document that matters. Even with harmless content the ability to build up a profile of usage and users to infer activity by combining that with other data is

a major privacy issue and potential security flaw.

Use Mattermost, Signal or Wire instead of WhatsApp. Owned by Facebook, WhatsApp produces a vast treasure-trove of meta-data and has a notoriously suspect record for data-privacy.

Get off Gmail and other commercial email services. Let us help each other get off GMail. No more sending around sensitive documents in GMail accounts. Use the privacy respecting ProtonMail or Tutanota instead.

Stop using Facebook and other commercial social media for anything strategic or sensitive. This should be done using Signal or Wire, or on UK Forums or Mattermost. Use air-gapping so that general information is on Mattermost or Forums, and specifics (such as car registrations, credit card numbers and addresses) is on Signal or Wire.

A Note on Passwords

When it comes to choosing a password, choose something which you can remember -- e.g. the initial letters of a phrase or line from a song that will stick with you, with some letters transposed to digit (o->0, I -> 1, to->2 etc) and a couple of uppercase and punctuation characters. The minimum length for a password is 8 characters and it should include both upper and lower case letters plus at least one digit and one symbol.

Do check that it is easy to type on all the keyboards you use -- mobile phones can make it a pain having to switch case, or switch between letters and digits, so you might want to have those grouped together in the password.

Don't rely on your device (or the cloud) remembering it for you -- there will come a day when you will need to actually type it because something has gone wrong. Ideally, keep all your passwords in a secure password manager (rather than giving them all to Google or Apple to remember).

Finally try to pick a password that you don't use elsewhere -- even if only by appending -xr to one of your standard passwords -- that will ensure that if your bank login gets stolen your XRUK ones are still ok and vice versa.
