PubHubs Position Paper

Authors: Bart Jacobs, José van Dijck
Version: February 1, 2023.

Introduction

Many civil society organizations, such as schools or public libraries, want safe online environments where communication and deliberation can happen *within* and *between* groups, and where identity management is a default affordance. For instance, a library may want to start a reading group for young members (age 8-12); a public broadcaster organizes content viewings for members only; or a school invites parents to join an online group when their children are on a fieldtrip. Libraries, broadcasters and schools now commonly resort to Facebook or WhatsApp because they have no safe and trusted online space as part of their public environment which is based on public values such as security, privacy, data protection, transparancy, accountability, and independence. They lack online environments that serve (locally managed) collectivity, rather than (global) connectivity; that offer connectedness within protected and private spaces when necessary. For this reason, we are in the process of developing PubHubs.

What is PubHubs?

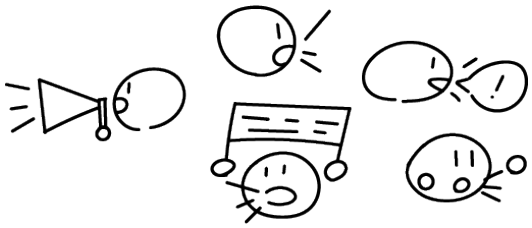
PubHubs (short for Public Hubs, see pubhubs.net) is an initiative started in 2022 in the Netherlands. PubHubs is not centered on individuals and their personal profiles, but on *public organizations* and their members as well as the publics they interact with. PubHubs offers its participants an online environment (“Hub”) for moderated conversation and trusted information exchange (text, audio, video, file exchange, calendars etc.) combined with digital identity management tools. PubHubs is based on open source software with a safe and secure architecture, responsibly governed by actual organizations and the communities they moderate.

A Hub is managed by an existing (brick and mortar) organization that works in the public interest and carries responsibilities towards its public, including a duty of care. Inside Hubs, organizations can shape their online space based on their own needs via so-called Rooms. Each Hub is expected to organize its moderation processes in accordance with its own norms and traditions. In the long run, PubHubs will also facilitate online interaction and communication *between Hubs* where communities can collaborate on projects, connecting individuals and professionals from various Hubs to pursue a common project. For instance, a group of fifty academics working at five universities engage in a research project and wish to create an enclosed online environment which allows them to work in various self-created sub-groups. Rather than starting WhatsApp groups or Mastodon instances for each purpose, they can use a protected and familiar online environment supported by their own organization.

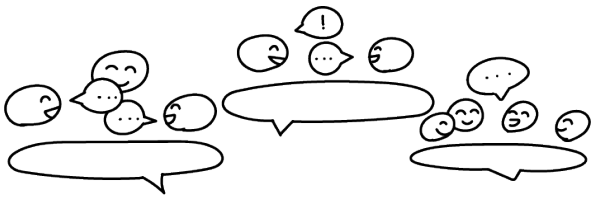
What is it *not*?

PubHubs is *not* an alternative for Facebook, Twitter, Instagram, WhatsApp or TikTok because it does not aspire to build a global centralized network for individuals. Social media platforms developed by the big tech companies (e.g. Facebook, Twitter, Instagram, Snapchat, TikTok) have allowed many people around the globe to connect and to express themselves: they enable family and friends in remote places to stay in touch with their loved ones and allow individuals (e.g. influencers) and advertisers to reach unprecedented audiences. Unlimited, global connectivity in a commercially driven online space is the default of mainstream social

media services. Participants present themselves via their own selfcreated profiles and are at the same time continuously profiled by the platform through their activities. Mainstream platforms are centrally operated and their services are paid for by targeted advertisements, driven by user data and profiles. The fact that users can communicate globally is attractive, but it also means that interaction is often unsafe and unprotected. Anyone can post anything, users can never be certain about the authenticity of sources or messages posted.



In recent years, we have witnessed the emergence of decentralized open networks, such as Mastodon, Matrix, and PeerTube, to serve as alternatives to centralized systems for microblogging (e.g. Twitter), social interaction (e.g. Facebook), or videosharing (e.g. YouTube). Their open source and not-for-profit character is a great improvement over mainstream social media, and their technical affordances offer more opportunities for self-moderation and self-organization. However, decentralized social media remain focused on offering (global) connectivity to individuals in an open, unbounded commercial-public space, making them vulnerable to some of the same problems as mainstream social media: unsafe communication, distrusted sources and malicious content. Mastodon users and developers are currently trying hard to improve their mechanisms for community moderation to enhance safety and control, which is an important development.



PubHubs does not aspire to replace existing social media; it also does not offer one super-tool as a solution to all major problems plaguing social networks (e.g. disinformation, identity fraud, grooming, etc). PubHubs seeks its own place in the online ecosystem where there is obviously a need for safe and secure spaces that support public organizations to work for and with their communities online.

For whom will PubHubs be designed?
PubHubs chooses to organize itself via local contexts, offering appropriate levels of privacy, protection and safety. In fact, it is an important aim of PubHubs to offer existing public organizations and institutions a reliable online space that facilitates their needs and reflects their offline identity and norms and while allowing them to interconnect. PubHubs aims to empower individuals *as part of a group* and communities *as part of a larger societal context*.

When designing a safe and trusted online environment (**Hub**) for a school, a public library, a patient self-help group, a public broadcaster, or a municipality, there are varying needs when it comes to communication. Within Hubs, conversations may be open to members of a group, rather than to everyone. Sometimes there is a need to post a message openly (e.g. to all

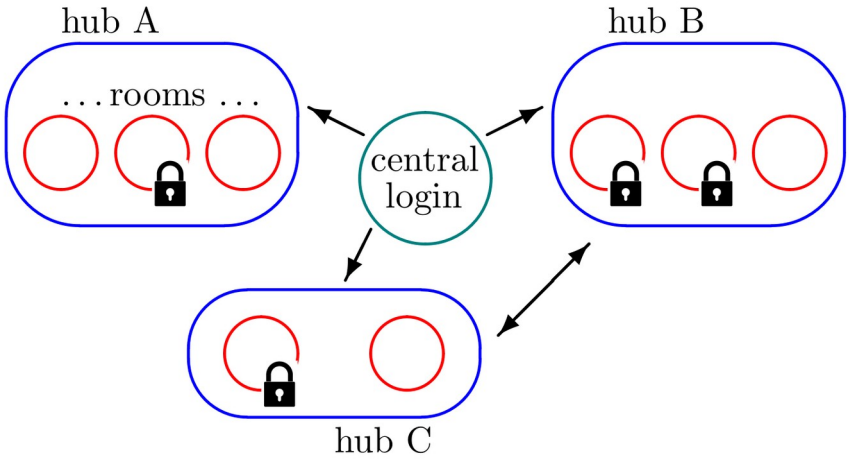
members of a Hub) but many organizations need smaller spaces with specific requirements for enclosed conversation, content exchange, or consultation with peers or professionals. PubHubs' architecture supports conversations within moderated contexts (**Rooms**). Hubs will typically present themselves to the outside world via a webpage that provides basic information about the Hub and its activities. This page contains a login button that takes users to the Rooms that the Hub offers. These rooms may (optionally) also have a public-facing website that provides information about what is going on in the Room and that may (in real-time) present a selection of its activities.

What makes PubHubs a safe online environment?
To provide a safe online space, PubHubs offers conversation and communication functionalities in combination with identity management and proportional, attribute-based authentication.

Identity management is an integral part of the PubHubs infrastructure for group-based conversation. The extent to which participants reveal their identity to others depends on the context. For instance, in a teaching setting the identity of students in a class will typically be visible within the group, for instance via their student identification number or simply via their real name. Another example is a patient group that facilitates a conversation about personal experiences with a particular disease; each patient's identity may be hidden via pseudonyms, while the authenticated expertise (and possibly registration number) of healthcare professionals should be known to everyone in the group. In other words, PubHubs provides participants (proportional) certainty about each members' identity, and thus supports the moderation of interaction, including conflict resolution.

PubHubs offers *proportional*, *attribute-based* authentication, so that participants know for sure whom they are talking to while only relevant, necessary identity information gets disclosed. *Proportional* means that authentication requirements are specific to each situation, and hence may differ in each context. *Attribute-based* means that users can be asked to disclose only relevant identity information—pieces of information such as their name, date of birth (or age limit), phone number, email address, profession, membership, etc.—in a specific situation. For each of the rooms, identity requirements may be different, and organizations and their communities can decide themselves which attributes are required in what rooms.

To guarantee a safe and secure online environment, PubHubs uses a central login as an entry point to all Hubs, as shown in the picture below. To register, users (currently) disclose an email address and mobile phone number as identifying information. PubHubs works with the identity app IRMA, but other 'wallet-apps' may be supported at a later stage as well—as long as they are open source, privacy-friendly and nonprofit. Once registered, users receive a PubHubs membership card in their IRMA wallet app on their phone, with their registration information. This card may be used for subsequent logins. Individuals' e-mail and phone data are not distributed to participating Hubs.



Once registered via the central login, users (participants) can proceed to any Hub. Once inside a Hub, they can move around the space that the Hub offers and view some general information, for instance about the Hub itself and what it offers. Organizations may facilitate various communities within the Hub to organize themselves. For some purposes, they may prefer small discussion or feedback groups with identified end-users while in other instances opening up interaction to wider (pseudonymous) audiences.
Users can join one or more Rooms where actual conversations take place. In each of these Rooms, different requirements for identification may apply. Hence, additional login may be required for particular Rooms within the Hub. For instance, within a school Hub, teachers may only allow registered students to enter their class Room. More generally, the administrators of such a school Hub can create special Rooms, not only for specific classes, but also for a particular group of students and/or their parents, for instance related to certain events.

PubHubs also uses this sophisticated identity infrastructure to allow users to move between Rooms. How does identity management work? After the central login, a user can visit any Hub. Upon visiting a Hub for the first time, the system chooses a random pseudonym for the user in that particular Hub, and uses this persistently when moving around within Rooms in the Hub. In principle, other people in the same Hub can only see this pseudonym, but a user may choose a more human-friendly nickname as well. When the user moves to a different Room, the pseudonym is automatically changed. Moving from one Room to the next, the different pseudonyms are automatically adapted by the system, for a smooth user experience. This happens consistently, so that re-entry of a Room happens with the same pseudonym that was used before.

Responsible governance and moderation
PubHubs is designed as a network of Hubs, each running their own online communities. Different organizations can run a Hub if they are part of the PubHubs network, support its public values, and accept a duty of care with regards to moderation and governance. Participating organizations commit themselves to taking responsibility for the proper organization and management of their online Hub. In particular, they are tasked with guarding trust and safety within their own Hub, to resolve conflicts, and to take down unfitting content —with ample space for their own culture, context, norms and (transparent) policy.
Moderation of content and communication is a serious commitment, not only in moral terms, but also in practical organizational terms, since it requires much time, effort and expertise. That's why it should be properly organized and guaranteed.

So how does moderation work within Hubs and between Hubs? Hub administrators typically create and manage Rooms within their own Hub, including moderation and access control, for instance, by including authentication requirements. Each Hub is responsible for appointing dedicated moderators for each Room. Administrators may allow users to set up their own self-moderated Rooms for collaboration and interaction, as long as they assign a responsible moderator. For instance, a cultural organization may set up a discussion Room about its latest exhibition, without any authentication requirements, so any PubHubs user who has entered via the central login can participate. But it may also choose to restrict access to such a discussion Room and require that people disclose specific attributes, such as their

membership (e.g. of a library) or real name (e.g. first name only) or age (rather than date of birth). It is up to the Hub administrators to approve specific authentication requirements for their Rooms. In the figure above, some Room circles have a closed lock, indicating such authentication requirements. When two Hubs cooperate, for instance, a school and a library, they may jointly organize an event in a Room that is assigned to one of the Hub-organizations involved.

Hub-administrators have the discretion to (temporarily) block a user's access from particular Rooms, or from the Hub entirely, if s/he seriously violates the Hub's norms and policy. At a technical level, this happens by banning the persistent pseudonym of a particular user from a Room or from the Hub as such. At the central login level, PubHubs-administrators can see which Hubs users are visiting, but they cannot track and trace user behavior inside Hubs. If they receive repeated notifications of misbehavior from different Hub-administrators about a particular user, they can decide to block him/her from entering the system altogether.

Cryptographically closed for Hubs, open for users
At the technical level, PubHubs builds upon the open-source conversation tool and standard Matrix. PubHubs has its own layers of digital identity around Matrix. It also has its own client, so that PubHubs' additional features, like authentication for (some) Rooms, can be optimally supported in its design. PubHubs is *open source*, but its network is *cryptographically closed*: participating organizations need to sign a contract in which mutual roles and responsibilities for governance are defined before receiving a secret cryptographic key that enables them to participate in the PubHubs network. Participating organizations run (or outsource) their own Matrix homeserver and are responsible for the data management within their own Hub. All data generated within a Hub remains on the (Matrix) server of that particular Hub and hence under the control of the Hub administrators. Data generated within one Hub are not accessible to other parties within the PubHubs ecosystem, including the central login, unless data are explicitly made public. Because of its cryptographically closed nature, PubHubs cannot be used with existing logins from other platforms, not even from Matrix itself; it would break the control and protection layer that PubHubs offers as key feature—for reliable authentication in Rooms and for digital signatures. PubHubs offers enclosed spaces but is *open* to everyone in their role as users, after entering via PubHubs' central login.

Short-term solution, long-term vision:
In the short term, PubHubs wants to offer a safe and trusted online environment for organizations; in the long run, PubHubs should become part of a public infrastructure of interconnected Hubs that allows users to move between Hubs. If a (large) number of organizations are going to use PubHubs software, there will be a need for joined activities online that move beyond the functionalities of current Rooms. For now, such inter-Hub collaboration can happen via Rooms operated by one assigned responsible moderator; in the future, cross-Hub activity may require a more sophisticated software design to make PubHubs a larger ecosystem of collaborating public organizations.

In addition, PubHubs may offer the future option to attach an (attribute-based) *digital signature* to *content* that organizations and individuals post. In this way both the message and source are authenticated, for instance, a message from the police or a health official. These digital signatures are part of PubHubs' innovative contributions to safety and security online.

Governance, co-creation, and research
PubHubs is run on a governance model that is not-for-profit. The nonprofit model still needs to materialize into a legal entity that oversees, maintains and runs the network at the central

level. Also, the process of decision-making is at the moment not yet formalized into a legally binding structure. Currently, PubHubs is developed by an expanding group of individuals and organizations, centered around PublicSpaces, a coalition of (semi-) public organizations in media, culture, education, healthcare and local government, and two research groups at the universities of Nijmegen and Utrecht in The Netherlands.

PubHubs functions as a co-creation project, which means that each participating Hub (public organization) supports the design process by contributing programming capacity to help shape its own Hub-space. In collaboration with the core PubHubs-design team and other participating Hubs, each Hub also articulates and develops its own specific needs and rules for moderation.

One of the larger aims of PubHubs, as part of the PublicSpaces coalition, is to research how to design and govern an online space driven by public values. Values such as safety and security have to be balanced off with at times conflicting values such as openness and inclusiveness, and each organization decides upon its own priorities As said before, PubHubs does not offer a one-size-fits-all solution for all online problems. Instead, it recognizes the need to negotiate public values contextually and to articulate what this tool can and cannot do for organizations. Designing the larger collective online space is a communal responsibility to which all participating organizations are asked to contribute. Therefore, the PubHubs design team organizes workshops to better understand the needs of public organizations not just in in relation to PubHubs, but also as part of a larger effort to rethink the online public sphere.

Conclusion

In sum, PubHubs offers a non-profit, open source and value-driven online environment for public organizations. It aims to enhance collectivity by strengthening civil society organizations and communities rooted in local and national connections, instead of promoting global connectivity, PubHubs wishes to co-create, together with its participating organizations and users, protected and managed online meeting places where people can safely interact, without data exploitation and profile-based manipulation. PubHubs is currently solidifying its basic architecture and infrastructure and plans to start prototyping in late 2023. Since it's a work in progress, this paper will be updated regularly in order to report and explain new steps.

Interested? Feel free to reach out via contact@pubhubs.net