Privacy Customization in a Social Sharing Tool

Where Academic Publications Meet Social Platforms

Julian Fietkau
julian.fietkau@unibw.de
University of the Bundeswehr Munich
Neubiberg, Germany

Laura Stojko
laura.stojko@unibw.de
University of the Bundeswehr Munich
Neubiberg, Germany

Abstract

Encyclia is a software tool to make ORCID records available on open social media platforms through the ActivityPub protocol. Through it, academic bibliographic information can gain additional visibility and interaction in the form of social posts, which raises new safety and privacy concerns. Advanced privacy settings on the Encyclia platform enable the personalization of information access and sharing. This paper discusses these privacy settings and systems as a case study for applying established personalization classifications from the academic literature. It differentiates implicit and explicit personalization via active user involvement and the dynamic role of the system itself in its purpose of bridging data across platforms.

CCS Concepts

• **Security and privacy** → **Privacy protections**; *Social aspects of security and privacy*; • **Information systems** → **Personalization**; • **Human-centered computing** → Social network analysis.

Keywords

privacy settings, social media, ORCID, personalization, adaptivity, adaptability

1 Introduction

ORCID[1] is a data platform where academics can set up a personal record to collect bibliographic metadata about their publications.

The Fediverse is a loosely defined network of interoperable social media platforms including Mastodon[2], Pixelfed, Misskey, and others. Fediverse servers allow users to follow one another to read and share content across servers by using the ActivityPub protocol [3].

We are in the process of developing a data bridge tool named *Encyclia*[3] that accesses ORCID publication data through the platform's open API and republishes it as ActivityPub data. This allows people on Fediverse platforms to follow individual ORCID records, receive new publications in their social feeds, and share them with their followers. As a source of open bibliographic metadata, ORCID (in contrast to closed academic platforms) is ideal for this purpose.

Bridging ORCID records onto social media platforms represents an interesting opportunity for personalization of the user's social feed. However, from the perspective of an ORCID record owner it also puts privacy concerns into focus, establishing a need for users to remain in control of what happens to their ORCID record through safety and privacy customization.

For the purpose of this paper, we treat Encyclia as a case study for real-world privacy customization on the borderline between two very different informational environments: ORCID and the Fediverse. This article provides an overview of the privacy issues that arise and the resulting design considerations for Encyclia's privacy and safety customization.

2 Privacy Settings on ORCID

ORCID record owners can use the ORCID website to make changes to the content or presentation of their record. This includes customization of which parts of the record are to be *public* or *not public*. In the ORCID context, "public" carries a specific meaning which is detailed in ORCID's terms of use[4], privacy policy[5], and privacy settings documentation[6]. Notably, public ORCID data is considered copyright-free and can be reused in other public and non-public contexts without specific permission or notice. This is a result of ORCID's purpose as a data repository for bibliographic metadata: to make its public data easily accessible and reusable by external systems and avoid duplicated data entry.

Most academics are eager to have their works widely shared and cited, as academic community reception is a major factor in career advancement. This group is well-served by ORCID's default privacy settings, which show metadata for all works publicly.

Some academics are indifferent about visibility, and some may even prefer to stay somewhat under the radar and keep a degree of close control over the visibility of their works [5], perhaps because they work in a field subject to political persecution or they are dealing with other sources of personal harassment. If they need to have an ORCID record (which is now mandatory for publishing in some venues), they may choose to adjust the privacy settings for all publications, including future ones, to be non-public. At the extreme end, an ORCID record can be "locked down" such that only the person's name and ID number remain publicly visible.

3 Privacy and Safety Concerns on the Fediverse

By making public ORCID data available via ActivityPub, we are simultaneously incorporating it into a new context with differing technical and social norms around data handling and introducing novel interaction modalities that ORCID does not provide on its own. The former is discussed in some depth in Fietkau [2] and will

---

[1]https://orcid.org
[2]https://joinmastodon.org
[3]https://encyclia.pub

---

[4]https://info.orcid.org/terms-of-use/
[5]https://info.orcid.org/privacy-policy/
[6]https://support.orcid.org/hc/en-us/articles/25538671642519

not be repeated here for the sake of brevity. This text will instead elaborate on the latter.

ORCID is intentionally designed not to be a social platform. Record owners cannot interact with one another on the ORCID platform; there are no facilities for sharing, commenting, or following. By bridging ORCID records into the Fediverse, Encyclia (a) makes ORCID record owners followable, (b) makes individual publications shareable, and (c) makes them open to comments and reactions, such as "likes". Each of these modalities needs to be considered from a privacy and safety perspective.

If an ORCID record is bridged through Encyclia and subsequently a new publication gets added to it, that record's followers can see it in their social feeds and may even receive a notification. This is not possible on the ORCID website – if one wants to learn whether an ORCID record has changed, the only way is to navigate to it manually and look. (ORCID does offer update notifications via its API, but this feature is exclusive to the highest membership tier reserved for academic institutions and their integrated systems. It is clearly not intended for individual users.) Even though in a technical sense Encyclia exposes no new information compared to the publicly visible ORCID record itself, the added modality of following and receiving update notifications may pose safety challenges related to, for example, stalking – an individual harasser that may have lost interest in checking an ORCID record for updates could instead be reminded by automated notifications.

Having individual academic publications be more easily shareable on social platforms is something that academics would likely broadly welcome, but that also poses privacy and safety questions. For example, on follow-driven social platforms where people with similar interests and values tend to follow one another, individual pieces of content can slip into "bubbles" of hostile or malicious users who may then proceed to attempt to cause harm to the author. Some social platforms give content authors control over who can see and share their posts, which can be used as a preemptive safety and privacy measure, and specific malicious actors can be blocked from interacting with someone's posts.

Lastly, social platforms often allow users to write replies or comments on specific posts, of which the original author may be notified. These can stimulate discussion and help establish new professional or personal connections, but they can also be a vector for abuse, such as cyberbullying.

With all of these new interaction modalities that Encyclia would introduce to ORCID record owners, its design cannot solely rely on the privacy customization offered by ORCID. Instead, it must provide privacy and safety customization options that take these additional concerns into account.

4 Privacy Settings on Encyclia

As established above, bridging public ORCID record data into social platforms introduces new interaction modalities which require safety and privacy personalization functions that ORCID itself cannot provide. For that reason, Encyclia has its own privacy customization interface, granting users access to additional customization.

To begin with, we note that the possibility of replies/comments from social platforms is a considerable safety concern that takes significant time and effort to moderate effectively. Encyclia preempts this danger by simply not facilitating replies or comments. Any text comments that arrive at Encyclia from other ActivityPub servers are quietly ignored and never displayed to ORCID record owners. Through this blanket decision, Encyclia renders replies/comments moot as a potential attack vector.

After authenticating as an ORCID record owner on the Encyclia website, the platform's account privacy personalization options become available, a portion of which is shown in Figure 2 (page 5). These include:

Account display customization: ORCID record owners can individually decide which descriptive parts of their record (biography, keywords, web links, email addresses, other identifiers) should be visible through Encyclia. Each one can be toggled on or off.

Server-based access restrictions: By default, ORCID records can be accessed via Encyclia from any ActivityPub server. If a record owner prefers to make their account inaccessible to specific servers ("block list" mode) or to restrict access exclusively to a specific list of servers ("allow list" mode), this is possible using the corresponding privacy settings.

Full opt-out: If an ORCID record owner would like to prevent their record from being bridged through Encyclia at all, a general opt-out setting is available that can be used without specific ActivityPub expertise.

Account deletion: For reasons of data protection, an ORCID record owner may elect to fully delete their bridged Encyclia account. In contrast to the opt-out toggle, this action is permanent.

5 Personalization Classification

Encyclia provides an interesting use case to observe and apply personalization classifications. The previously described characteristics of the application and its privacy settings are being mapped to the adaptivity and adaptability degree defined by Oppermann et al. [4] in addition to the classification scheme by Fan and Poole [1], which distinguishes explicit and implicit, individual and categorical personalization such as four design paradigms: architectural, instrumental, relational, and commercial. To determine which aspects of Encyclia align with these classifications, both authors collaboratively derived suitable assignments. One researcher proposed an initial classification and documented the rationale based on system behavior and examples. The second researcher, who contributed domain-specific knowledge of Encyclia and its differentiation from ORCID, critically reviewed these assignments and provided refinements. Discrepancies and out-of-scope classifications, not referring to privacy settings, were discussed until consensus was reached.

The first perspective concerning personalization focuses on the user involvement and degree of adaptivity when transferring publications from ORCID through Encyclia and making them available on social media. Categorizing system design and customization possibilities in the spectrum of adaptation by Oppermann et al. [4] provides an interesting approach to view the solution from a personalization perspective. Mapping the previously described privacy settings to the adaptation spectrum [4], we can distinguish two extremes realized by Encyclia:

(a) Default – implicit personalization by categorical privacy settings from ORCID

(b) Customized – explicit personalization by individual privacy settings on Encyclia
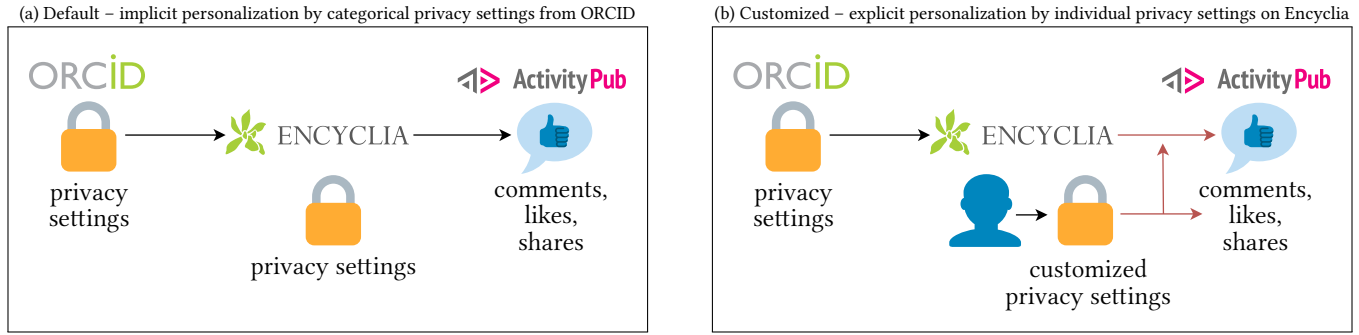

Figure 1: Overview of two personalization classifications of Encyclia showing (a) the default with implicit personalization by carrying over the privacy settings of ORCID, and (b) the explicit personalization with user customization of privacy settings initiated by users on Encyclia that impacts the transfer via ActivityPub.

- Adaptive – no user control: The functionality of Encyclia is enabled by default and makes ORCID records available via ActivityPub without the user's interaction. Interestingly, the users do not need to be specifically registered with Encyclia, which enables it to perform its service without any user intervention and control, even performing the data translation without their knowledge (as ORCID users have given permission by agreeing to the ORCID terms of use).
- User-initiated adaptability, no system initiation: To counter potential harm social media can cause by including ORCID records in users' feeds, Encyclia provides user-initiated adaptability to their privacy settings, managing the transfer of their data to ActivityPub. This includes: display customization, block list / allow list settings, full opt-out, and permanent account deletion.

For further details, the second personalization perspective classifies the different privacy settings and features into the classification scheme and design paradigms of Fan and Poole [1] for personalization systems. Before summarizing the result and discussing design paradigms, the three questions for classification [1] are discussed:

What is personalized? The objective of the personalization is to focus on the privacy settings of ORCID users concerning the transfer of their data via ActivityPub by Encyclia. This type of personalization objective focuses on the *information access* to the ORCID records displayed on ActivityPub.

To whom to personalize? The personalization via privacy settings focuses on *individual* ORCID records, and by default, Encyclia uses *categorical* personalization to decide on the degree of personalization based on the privacy settings of ORCID records. For example, in case an ORCID account is mainly private, the publications of this account are also not forwarded to the Fediverse by Encyclia. All public information is assumed to be intended as open and forwarded by Encyclia as default functionality without additional restriction.

Who does the personalization? In this respect, the default settings are the *implicit* personalization enabled by Encyclia without user interactions, as discussed with the adaptation spectrum of Oppermann et al. [4]. However, the personalization transforms

into *explicit* personalization through user customization by Encyclia's optional privacy settings. This enables users to retain control over their ORCID records and how they are used in social media platforms by restricting data transfer or access.

Figure 1 displays the interplay between (a) Encyclia as an adaptive system with automated personalization using implicit categorical preferences from original ORCID records for information access to (b) Encyclia as an individually personalized transfer service through explicit user customization of privacy settings for information access, in addition to previous ORCID settings. This default use of ORCID privacy settings enables seamless personalization that aligns with users' original sharing intentions, offering a meaningful baseline before any further customization.

Additionally, to these classifications of user involvement and personalization degrees, the design paradigms of Fan and Poole [1] provide an additional perspective on the privacy settings of Encyclia. While commercial and architectural paradigms are not the focus of such settings, the personalization is more strongly related to instrumental and relational aspects.

Instrumental personalization. The provided privacy settings enable additional functionalities that support the user's preferences concerning the transfer and access to their ORCID records.

Relational personalization. Transferring ORCID records to social media platforms through ActivityPub fosters social exchange and increases visibility of the person's work. Encyclia's additional privacy settings enable users to customize their individual needs for socialization and sense of belonging, which may differ from the default setting by restricting access to their information.

In this discussion of personalization classifications for the case study of Encyclia, we observe a pattern of dynamic transformation between personalization degrees, where the system transitions between modes, such as implicit to explicit and categorical to individual personalization, depending on user interaction and involvement. This illustrates how privacy settings in such systems are not fixed, but can shift responsively according to user preferences. Increasing user customization thus becomes a vital aspect of future development to handle privacy concerns in systems that republish open data. Encyclia exemplifies a novel case of dynamic transformation in privacy settings. While existing classification theories typically

handle personalization types as static categories, our analysis emphasizes the importance of supporting fluid transitions, particularly as data practices and data portability rights grow in prominence, while users' privacy needs remain diverse and context-dependent. Enabling user customization can address the nuanced trade-offs between visibility and privacy.

6 Outlook and Conclusion

In this paper, we have investigated personalization classifications and how they relate to the use case of Encyclia and its implementation of privacy settings concerning the transfer of ORCID records via ActivityPub, making such records available on the Fediverse. With the sharing of bibliographic data to these platforms, additional social features such as comments and likes become available that extend the previous intentions of ORCID, and consequently, they require additional privacy features to enable authors to control their records more precisely. With this functionality, Encyclia moves beyond implicit personalization via categorical privacy settings taken over from ORCID settings to a system that enables users' adaptability with explicit personalization through individuated privacy

settings. In the future, the system may incorporate additional features for certain settings to enhance the decision-making process by, e.g., recommended allow-lists for servers or auto-completing functions in text fields, leading to more differentiated interaction beyond the extreme ends of the adaptive/adaptable spectrum.

References

[1] Haiyan Fan and Marshall Scott Poole. 2006. What Is Personalization? Perspectives on the Design and Implementation of Personalization in Information Systems. *Journal of Organizational Computing and Electronic Commerce* 16 (2006), 179–202. Issue 3-4. doi:10.1080/10919392.2006.9681199

[2] Julian Fietkau. 2025. ORCID and the Fediverse: What Can We Do with Public Information?. In *EUSSET Conference on Computer-Supported Cooperative Work (ECSCW) 2025*. European Society for Socially Embedded Technologies (EUSSET), Siegen, Germany, 7 pages. doi:10.48340/ecscw2025_pd04

[3] Christine Lemmer-Webber, Jessica Tallon, Erin Shepherd, Amy Guy, and Evan Prodromou. 2018. ActivityPub. W3C Recommendation. https://www.w3.org/TR/activitypub/

[4] Reinhard Oppermann, Rossen Rashev, and Kinshuk. 1997. Adaptability and adaptivity in learning systems. *Knowledge transfer* II (1997), 173–179. doi:10.24406/publica-fhg-191910

[5] Jaime A Teixeira da Silva and Quan-Hoang Vuong. 2021. The right to refuse unwanted citations: rethinking the culture of science around the citation. *Scientometrics* 126 (2021), 5355–5360. Issue 6. doi:10.1007/s11192-021-03960-9

Who should be allowed to access your account?

Decide who is allowed to read and interact with your Encyclia account: by default, the content of your account can be accessed from anywhere. You can use the following settings to block a subset of Fediverse servers from accessing it, or to restrict access to specific servers.

🔘 **Public**

Your Encyclia account is available publicly and anonymously, through ActivityPub and on this website.

⚪ **Block list**

Your Encyclia account is not available anonymously via ActivityPub, requests for it must be signed ("authorized fetch"). Servers on your block list will be unable to access it. Your account is still available to anyone reading it anonymously on this website.

Your block list:

⚪ **Allow list**

Your Encyclia account is not available anonymously via ActivityPub, requests for it must be signed ("authorized fetch"). Only servers on your allow list will be able to access it. It is additionally hidden from anonymous access via this website.

Your allow list:

Block/allow list format: one server per line, listing only the host (e.g. "example.social"). Entries that are still displayed after this page has been saved and reloaded are formatted correctly.

Note: all information shown on your Encyclia account comes directly from your ORCID record and is marked as "Public" there. If you have concerns about any of this information being accessible, Encyclia recommends making use of ORCID's privacy settings to restrict access as needed. Note also that posts generated by Encyclia are addressed to the public in the ActivityPub sense, meaning that other servers are technically allowed to share them to anywhere else in the network.

☐ **Opt your ORCID record out of Encyclia**

This setting fully opts your ORCID record out of being bridged into the Fediverse. If your account has never been requested through Encyclia, this opt-out will prevent it from being created. If an Encyclia account was already created for your ORCID record, it will be deactivated and your personal information will be removed. Deactivating your bridged account will immediately remove all existing followers. You can come back here later and reactivate your account if you change your mind, but previous followers will not be reinstated.

▶ Account data export or deletion

Figure 2: A portion of the current privacy customization settings in Encyclia, accessible by authenticating with an ORCID iD on the Encyclia website. This section shows the options for account content access restrictions and for opting out of Encyclia. The section for customizing which ORCID record fields are visible on Encyclia is omitted to fit the page.