Identity Leakage Deep Dive

Confidential
As of 4.14.2023
POC: [redacted], Privacy Policy

Overview: Identity leakage

Meta users can have multiple accounts across our Family of Apps (FoA). We know some users want to link their FB, IG and Meta accounts, while others prefer standalone accounts. Whether for an influencer who wants to cross-post automatically across Facebook or Instagram, or a person who must keep a marginalized identity private on a secondary profile, it's important that users understand and control the visibility of their online personas.

What is identity leakage; what is doxxing?

Identity leakage is the unintentional exposure of personal information online. At Meta specifically, the issue arises when users' multiple accounts are inadvertently revealed – without the user's intent to do so.

The related concept of **doxxing** is the intentional act of publicly revealing someone's personal information without their consent; doxxing also entails leaking a user's identity, but with the intention to harass or cause harm to someone else. [HYPERLINK "https://onlinelibrary.wiley.com/doi/full/10.1002/9781119429128.iegmc009" \h] suggest women are more likely to be targets of doxxing.

What causes identity leakage and doxxing? What can we do about it?

Identity leakage may occur as a result of:

1. **Meta product behavior** (e.g. we recommend a person's secondary profile to their primary profile's friends)
    a. In cases where Meta product behavior is the cause, we need to identify the risk, understand the scope, and then devise and implement *product solutions*.
2. **Users' lack of awareness and misuse of a product** (e.g. a user accidentally shares a IG Story with everyone when they intended to share it with just Close Friends.)
    a. In these cases, we need to *give users information* about our products that will reduce the likelihood of unintentional disclosures.

Doxxing typically occurs as a result of:

1. **Users with malicious intent** who manipulate our products to target users.

a. ID leakage can lead to doxxing by making it easier for malicious users to doxx.

Meta has worked to address both product design and user education; in some cases, we have worked on engineering solutions to improve product functionality. In others, our focus has been on enhancing transparency and investing in user education. As we strengthen the connections between the FoA, we need to identify gaps and solutions in each category.

What are the consequences of identity leakage and doxxing?

Both identity leakage and doxxing can lead to serious, offline harms, [HYPERLINK "about:blank" \h] reputational damage, threats, stalking, and fraud. Moreover, lawmakers and regulators often scrutinize social media product behaviors that can enable ID leakage/ doxxing (e.g. Meta has been asked by the FTC what risk mitigations were in place to prevent identity leakage/ doxxing and additional Facebook profiles [SOAPs].)

The following summarizes (1) Meta product features that may lead to ID leakage and/or doxxing, (2) the current protections we have in place to prevent ID leakage, and (3) how some of these issues and protections may evolve in Future 3 when users have Meta accounts with FoA profiles.

1 – Product features that may enable ID leakage

I. **Friending and Following Recommender Systems (People You May Know, Accounts You Should Follow, etc.)** (Cause: Meta product behavior and/or lack of user knowledge)

Friending and follower recommender systems may enable identity leakage due to a range of product behaviors and/or users' misunderstanding and misuse of the products. For instance, ID leakage risks have been raised in the context of SOAPs and PYMK; as such, we have taken precautions to separate a SOAP and Main Profile's social graph (see more in Section 2.VI). We also know it is possible for users to enable continuous contact uploading in multiple, unlinked accounts and intertwine their social graphs (see more Section 1.IV). Although there are multiple ways users can experience identity leakage and doxxing via PYMK/AYSF, the most serious and acute risk is a product behavior known as *soft-matching*.

Soft-matching occurs where data is used to match the same user across two different Family of Apps accounts without user permission. Due to regulatory action, we are deprecating inter-app soft matching. (See the [HYPERLINK \l "bookmark=id.63oaarpkfyqb" \h]) Before its deprecation, however, features like PYMK and AYSF could cause identity leakage by recommending user accounts across platforms when the user intended to keep those accounts as separate identities.

For example, if a user has a Facebook account, "FB1'' which represents their 9-to-5 persona, and an Instagram account, "IG1" for their gamer persona, the FB1 profile might surface as a

Commented [1]: For this audience, I think it's worth separating intRA and intER mitigations, because they've now diverged.

These risks came up earlier and with this FX audience when we did MANI. In that time, with Identity Sync still being plan of record, we had a very strong mitigation to avoid traversing AC links that weren't IS links inside graph retrieval... that way graphs couldn't be mixed between profiles.

When we deprecated use of IS links for PYMK / AYMF, we must have dropped these mitigations. So, I think the intER-app mitigations are now a notch weaker than the intRA-app mitigations.

Commented [2]: Nit here: I see usage of AYMF and AYSF in the doc. Are they the same product?

Commented [3]: I'm not sure this is true. It's maybe the least visible risk, but I would've guessed the most likely risk is user "error". It's gotta be hard to use a secondary profile and never make an explicit action that connects profiles, like friending someone in the main graph or commenting on a main friend's post, etc.

Commented [4R3]: I think all 3 may apply for softmatching.
1/ most serious -- due to commitments we have
2/ least visible -- I think the detectors that company may have possible chance of slipping detection (as it's not perfect yet).
3/ most complex -- triaging and verification proved to be so hard.

Commented [5R3]: But I think what Ashwin is trying to capture is that in general the most concerning issue would be:

1/ user error -- of comingling graph with Main Profile due to lack of knowledge or mistakes
2/ softmatch error -- of systemic error or engineer error of comingling data across accounts

Commented [6R3]: To clarify, I'm specifically referring to doxxing risk. Agreed that SM is critical for commitments, lack of visibility, eng cost, etc. But specifically to the point about what's the most likely reason for doxxing, I think it _might_ be accidentally co-mingling by user actions.

It's just a guess though. I wonder if we've done deeper UXR here before.

PYMK recommendation to IG1 followers also on Facebook; conversely, the IG1 gamer profile may surface as a AYMF recommendation to FB1's friends on Instagram.

Note that we almost entirely [HYPERLINK \l "bookmark=id.pqclguu8kpee" \h]*across* apps, known as inter-app soft-matching. However, we have not yet remediated intra-app soft matching on Instagram to the same degree.

Lastly, while soft-matching heightens the risks associated with PYMK and AYSF, identity leakage and doxxing risks persist even in the absence of SM.

II. **Groups You Should Join and other Account Recommender Systems** (Cause: Meta product behavior/ Lack of user knowledge)

Like PYMK and AYMF, Groups You Should Join (GYSJ) is a recommender system that delivers personalized group recommendations to users. GYSJ may lead to identity leakage in a few different ways. Some users with multiple accounts may join the same group; if the membership list is visible to the public, the shared identity may be discovered. And whether the group is private or public, the Group admin would see both account members in either case. Some Groups also have a feature called "Anonymous Posting," which is not technically anonymous since Group admins also see the poster.

Commented [7]: nit: this wouldn't be soft-matching. Maybe it needs another phrase to precisely separate the leak patterns... self-doxxing maybe?

It is also possible the soft-matching and group recommendations contribute to identity leakage – although more research is needed to confirm. For instance, although GYSJ does not recommend individual users, it still recommends groups, some of which are public and whose members can be seen. Imagine a user has IG1 and IG2 profiles that are soft-matched; their IG1 account is hardlinked with a FB1 profile, and the FB1 profile is a member of X Group. A hardlinked FB friend who follows the IG2 profile may receive a recommendation to join X Group and, if the group is public, may see the list of members and find the FB1 profile.

Commented [8]: There's also an inverse of this unit called PYMI - People You May Invite. It's supposed to target group members to invite people (their friends) into a group.

Although the deprecation of inter-app soft-matching mitigates this risk, it may still exist due to the possibility of intra-app SM.

Lastly, note that further research is needed to understand the extent this risk may exist with other products, such as Search and Tagging. Both Search and Tagging Photos also used personalized recommendations to surface user accounts, much like PYMK or AYSF. For example, a user's IG1 - IG2 accounts are soft-matched and both are public. Not only is it possible for IG2 to be recommended to an IG1 follower ("F") via AYSF, but if F clicks on a photo to tag, IG will show a personalized list of followers and non-followers F may wish to tag. It is possible that IG2 is surfaced to F as an account to tag, much like with AYSF.

Commented [9]: Do we know if Search/Tagging/etc are doing some sort of doxxing protection like PYMK? We should be able to do that at least for intER app matching where we know the profiles can't represent the same identity.

Commented [10R9]: I'm not too sure, but is it possible that these products may be using PYMK directly?

III. **Account Center and ID Sync** (Cause: Lack of user knowledge)

Commented [11]: We cover ID sync, but should we also cover basis on what it means to add account in AC (Commonly known as hard linking or account linking or account center link, etc).

If someone uses their Facebook and Instagram profiles for different purposes (i.e. professional and personal), their profile might be recommended to unintended audiences. Therefore,

Commented [12]: Are we still investing in ID sync? We already dropped this from PYMK / AYMF, so curious if we're going to come back to ID sync or build some replacement.

Account Center offers a user an option to "Identity Sync," which syncs a user's name across accounts. This makes users discoverable across apps.

For example, the image below shows two users who have added their FB and IG accounts to AC and opted in to Identity Sync. This will likely lead to appearing as recommendations to friend/follow in the other app.

Commented [13]: Would like to better understand what this means, is there product functionality that makes them more discoverable? I always thought this value prop was conceptual/utilitarian. Ex: If I know your name is Anne Smith on FB, I would likely search for Anne Smith to find you on IG

Commented [14R13]: When you opt into Identity sync, not only are your fields syncable across apps, but your other profile is eligible to be recommended to your friends.

Commented [15]: There is no image here, is this referencing page 6?

IV. Contact uploading and contact points (Cause: Lack of user knowledge)

What is contact uploading? What are contact points?

On both Facebook and Instagram, users can upload contacts from their devices address book to find friends/accounts to follow more easily. The phone numbers and email addresses stored in a mobile device's address book are matched with accounts of users that the device owner may know. Once users opt-in to this feature, the upload occurs at regular intervals – known as continuous contact uploading ("CCU"). [HYPERLINK "https://fb.quip.com/1glNAnTld1od" \h] or AYSF candidates. Note that although only some users utilize CCU, all users have some contact points tied to their account, such as email addresses and phone numbers.

Moreover, CCU also employs "[HYPERLINK "https://www.internalfb.com/launch_manager/reviews/L1056915PRV/Finish" \h]," a contact graph based on users' phone number address book and users' previous and confirmed phone number. ID2ID uses Instagram and Facebook address book data to make inferences about the relationships among address book imports. Specifically, ID2ID precomputes inferences such as (i) which users uploaded a declared contact (direct import) and (ii) which users uploaded that same declared contact into their address book (reverse import). ID2ID only uses address book data for contacts that have been declared by the importee.[1]

Can contact uploading/ contact points lead to identity leakage?

While the products (CCU, ID2ID) themselves do not necessarily lead to identity leakage, users may not understand how CCU and ID2ID affect cross-app friending and following recommendations. For instance, a user might utilize CCU for separate (non-connected) FB and IG accounts – or users may list similar contact points for multiple accounts, placing them in a similar social graph. As discussed in Section III, Meta will likely need to plan how CCU will function under Future 3, when users have Meta accounts with FB, IG, etc. profiles.

Commented [16]: This is a good callout and shows up in the account v profile data doc here: https://docs.google.com/document/d/1PQjJimWLD-vzUzUv-puNNaKrsFdU1qlfkfRi_vxU85k/edit?disco=AAAAvDBBelo.

Even if contact points exist at the account level, there would need to be a way to selectively decide where contact graph is used for a profile.

V. Location sharing (Cause: Lack of user knowledge)

Facebook and Instagram allow users to share their location in their profile as well as to mark individual posts as taking place at specific locations. In conjunction with other ID leakage features, unintentional location sharing can be used for doxxing (confirming two accounts are

[1] ID2ID does not use inferred contacts or perform soft-matching. ID2ID serves as the single choke point for respecting contacts' privacy requirements.

concurrently at the same location.) Once again, while the product itself does not necessarily lead to identity leakage, it is a feature Meta has factored into its ID leakage protections, as discussed in Section III.

VI. Visibility (Cause: Lack of user knowledge)

If users do not understand how to manage their visibility controls, they may accidentally overshare information. A few of these include:

1. The visibility of their **profile information** or **profile** itself (e.g. whether a user understands how to share where they went to high school with Only Me or Everyone; setting an IG profile to private or public)
2. The visibility of their **posts** (e.g. whether a user understand how to share Story with only Close Friends)
3. Their **active status** (e.g. users may not understand how to turn their active status off; this is visible status that, like location sharing, can be used to suggest or confirm that multiple accounts are shared by the same owner)
4. Whether their **views** are visible (e.g. whether a user understands that when they view a Story, the poster can see who viewed their post)
5. Profile switching (e.g. do users understand from which profile [and thus with which audience] they are sharing content?)

2 – Current protections against ID leakage at Meta

The following covers the significant steps Meta has taken to protect users against identity leakage and doxxing. However, it should be noted that these steps have not "solved" ID leakage risks, and additional recommendations for further improvement are covered in Section 3.

I. Deprecating soft-matching

Meta's Cross App Soft-Match Deprecation (CASD) initiative is a company-wide effort to (1) discovered account soft-matching occurrences, (2) remediated those identified use cases, and now (3) enforces and monitors these efforts to prevent future cases of soft-matching from occurring. For the latest developments on this work, see the [HYPERLINK "https://fb.workplace.com/groups/736394813693281" \h].

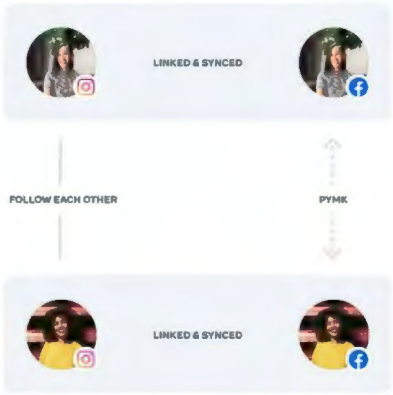
II. Account Center and ID Sync

Today, instead of soft-matching accounts without users' knowledge, users **opt-in** to cross-app data usage and combination by adding their accounts to [HYPERLINK "https://about.fb.com/news/2020/09/privacy-matters-accounts-center/" \h] (launched in 2020.) While we tell users that we use information across our apps to personalize their experience and show more relevant content, we also state that using Account Center does not necessarily

mean they need to have the same identity across all our apps. ("You can still choose to be Aisha Ahmed on Facebook, for example, and @bakersdozen on your Instagram account.")

Therefore, Account Center offers a user an option to "Identity Sync," which syncs a user's name across accounts; users typically opt for ID Sync when they *want* to be discoverable across apps.

For example, the image below shows two users who have added their FB and IG accounts to AC and opted in to Identity Sync. This will likely lead to appearing as recommendations to friend/follow in the other app.



When a user adds their accounts to Account Center, it does *not* mean linked users will not be recommended to cross-app friends/followers, or won't receive cross-app recommendations.

With that in mind, while Identity Sync is intended to [HYPERLINK "https://docs.google.com/presentation/d/1c49EizZjEk4YpDRWh0QhaVIqdY3hzPs1jxX1AIGKrgo/edit" \l "slide=id.g144d14c5ce8_0_0" \h] leakage, Policy believes it is ultimately **an inadequate solution** that does not give users the information and tools they need to manage their online identities.

III. Personal information visibility control/ profile visibility control

Facebook and Instagram give users various controls over how public or private certain profile information is. For instance, Instagram allows users to keep their profiles private, while Facebook only allows users to designate audiences for certain pieces of profile information (i.e. Users can share where they went to college with the Public, Only Friends, Close, Only Me (private), etc.). These visibility controls ensure users can choose how widely available they want their profile information to be. When users have the option for a more private profile experience, it reduces the chances of doxxers accessing their personal information.

IV. Profile switching, audience management, and post visibility

Commented [17]: It is not clear to me if we intentionally use Profile Sync signal to drive friending recommendations? If I choose to sync my FB<>IG profiles, does that mean my FB profile will go into the pool of recommendations for my IG followers, and vice versa?

Commented [18R17]: Also to note, I believe we do not describe cross-app friend recommendations outside of AC disclosures. It is not explicit in the UI that opting into profile sync enables cross-app friending recommendations, if that is what is happening

Commented [19R17]: If I choose to sync my FB<>IG profiles, does that mean my FB profile will go into the pool of recommendations for my IG followers, and vice versa?

Yes this is true I believe

Commented [20R17]: I agree, IIUC, Identity (Profile?) Sync is required for you to be recommended as PYMK of AYMF candidate.

Though I don't think there is any disclosures at IS time that describes this information.

Commented [21]: Can we tighten up this for clarity? I'm not sure I understand.

Commented [22R21]: +1

Commented [23]: can we link to the reasoning here or put it in the doc?

Commented [24R23]: +1

Commented [25R23]: Does this mean Policy does not believe this resolves the risk for people or is it not defensible for regulators?

Commented [26]: This discrepancy could be confusing in registration or syncing experiences. For example, let's say I want to leverage my Meta account and IG profile to get started with a new profile on FB. If my IG profile is private, I would expect a FB profile created and synced to that IG profile to be private also.

FB and IG also give users post visibility controls (e.g. sharing a Story with only Close Friends). This ensures they have the option to control who can see their posts, photos, and other content.

Another important aspect of audience and post visibility management is ensuring users know from which profile they are posting. Since we introduced cross-app Switcher in 2022, users have been able to seamlessly switch between FB and IG profiles. Knowing which profile is being used for posting helps ensure that content is shared with the intended audience (i.e. whether it's from a personal or professional persona), reducing the risk of accidental exposure of sensitive information.

V. Cross-App Notifications and Post Views

Commented [27]: This is a great example with what the remediation was. It's really hard to think through these corner cases. Is there a framework people could leverage to see if new features or experiences may unintentionally lead to identity leakage?

Cross-app PXFN's continue to ensure protections against doxxing in cross-app products. Most recently, the cross-app value (XAV) PXFN saw a proposal to notify hardlinked IG-FB users when they are tagged in an IG → FB story. In this instance, when an IG user is tagged in an IG post, and that IG post is cross posted to FB, the XAV product would notify the tagee on FB. A bad actor could use "clean" accounts (no friends, followers) to target an IG account, cross-post to Facebook, and then check which FB users have viewed their FB story. However, the PXFN ensured that only taggers who are Facebook friends with the tagee can see who viewed their story. As more cross-app features are launched, PXFN's continue to ensure anti-doxxing protections with each proposal.

VI. Single Owner Additional Profiles (SOAPs)

SOAPs allow users to create multiple profiles on Facebook. With the creation of SOAPs, we introduced various protections against identity leakage, including transparency, controls, and default limitations. See [HYPERLINK "https://docs.google.com/document/d/1iMBefgmkGN9MUS6WdqIqDPZm3ay5Nk2t/edit?usp=sharing&ouid=102428276809283502179&rtpof=true&sd=true" \h], and highlights below:

- We ensured Account Settings will be accessible only when switched into the Main Profile. Centralizing where users can access settings helps prevent accidental exposure.
    - When accessing SOAP settings, a disclaimer indicates that the settings "Control preferences for this profile like privacy, notifications, and other settings."
- There are special protections for [HYPERLINK "https://fb.quip.com/1glNAnTld1od" \h].
- SOAPs do not have access to messaging threads in the Main Profile or other profiles when switched into the SOAP. This prevents users from accidentally messaging one of the main profile contacts from their SOAP persona, accidentally revealing their identity.
- Location History is set at a profile level to minimize mixing on-site signals across profiles.
- Active Status will be enabled at a profile level with options of on or off, and default is on.

Commented [28]: FYI I'm working with the SOAP team to bend these rules we put in place years ago. They're trying to use some MP signals to grow AP engagement to help with cold start recommendations. More info here: https://docs.google.com/document/d/1CXWDfRJUnDS53x_RD0vgZvpQc5NITdXsY7vQqsO0go4/edit#

- SOAPs cannot access device contacts to find profiles because it will not have contact uploader enabled. This prevents the SOAP and Main Profile from sharing the same PYMK recommendations based on contacts.
- Under the setting How People Find and Contact You, phone number and email options for SOAPs will be set to Only Me and not editable to prevent any profile from discovering a SOAP based on a direct or inferred contact point.
- **Soft blocking.** Blocking is per-profile (i.e. if A blocks B, A does not block any of B's other profiles); however, the block triggers additional soft measures (i.e. blockee can message or initiate contact with blocker's SOAP.) Soft blocking helps prevent the blockee from deducing that the blocker's Main Profile and SOAP belong to the same person.

3 - Recommendations for Future 2 and Future 3

The following are recommendations of ways to mitigate risks of identity leakage and doxxing via Meta products. Many of these apply equally to our current products (Future 2) as well as our future account model (Future 3.)

Our recommendations are summarized as follows:

1. **Investigate the scope and potential risk of intra-app soft-matching**
2. **Improve or rework Identity Sync**
3. **Create a cross-app friending and following discoverability control ***
4. **Streamline and improve friending and following transparency and controls across apps**

*(We consider a cross-app friending following discoverability control to be *the most important step* we should take.)

Commented [29]: I think this was one big IntraApp mitigation for SOAP.

Shall we rephrase this to say that SOAP cannot be associated or found with any Direct/Inferred/Reverse Contact Point by 1) system design that SOAP are incapable of owning or associated with any CP and 2) settings set to "only me"

Commented [30]: Have we considered an ML-based approach to inferring identities? SOAP is going down this route, and it might help with users having to deal with less cognitive load, and us getting "good enough" guesses to inform UX flows for upside and privacy scenarios where we're trying to prevent downside.

https://docs.google.com/document/d/1CXWDfRJUnDS53x_RD0vgZvpQc5NITdXsY7vQqsO0go4/edit#heading=h.9qybcz3mrs42

Commented [31]: We have done some explorations around moving friending recommendations to be behind an AC setting instead of identity sync. Currently it is not planned to be executed on

Commented [32R31]: Is there a link to more info here? I thought we already removed the IS dependency in PYMK/AYMF and moved to just AC links?

Commented [33R31]: e.g. https://fb.workplace.com/groups/141679713188761/permalink/1112201306136592/

Commented [34R31]: We still have IS required for *profiles to be recommended as PYMK Candidate*. I think this is what Daryl may be referring to.

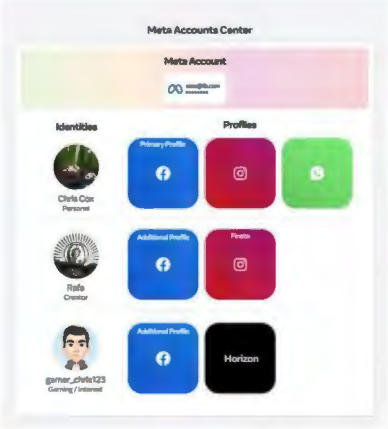
IIRC, pXFN showed concerns in removing IS for above scenario.

[redacted]@meta.com We've talked about above in chat. But do we have any documentation of this decision and next steps?

Commented [35R31]: Yup good clarification. That's also consistent with how SOAP p-xfn are encouraging MP signals for the AP as viewer, but not candidate.

On a related note, is this group invested in the use of hard-links vs IS links being consistent across teams? I'm not sure AYMF made the same viewer v candidate distinction (just haven't checked yet). And I'm also not sure if the platform teams (id2id, closeness) have made the same
choices: https://fb.workplace.com/groups/1023758544867062/permalink/1345107672732146/.

As we move to Future 3 – where current FoA *accounts* in Account Center become *profiles* under a Meta account (see graphic below) – the risks of ID leakage and doxxing may become exacerbated by a more complex account structure.



Commented [36]: This could potentially flip, imo. If we're able to introduce an identity-level concept under accounts, this actually creates the opportunity for stronger mitigations than we'd be able to do otherwise.

When a user links an account and doesn't identity sync, that gives us extra knowledge to filter from pymk/aymf/search/etc so that we help ensure the user doesn't mix their signals/graph and reveal themselves. We wouldn't be able to do that without AC. This could actually be a privacy value prop, if we can make IS links or something like it more adopted.

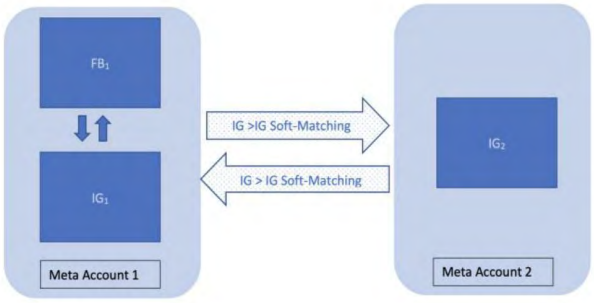
I. **Investigate the Scope and Potential Risk of Intra-App Soft-Matching** (Meta product behavior)

We know that intra-app soft-matching may be currently occurring on Instagram. This not only presents current risks, as covered in Section 1, but will also pose risks to users and our FCO compliance when we transition to Future 3.

Current intra-app soft matching may lead to Meta-to-Meta account (MA<>MA) soft matching in Future 3. This can occur when two intra-app accounts that sit in different Meta accounts are soft-matched. For example, if a user links a Facebook and Instagram profile (FB1 and IG1) in Meta Account 1, and also keeps a second Instagram profile (IG2) in its own Meta Account 2. In this case, data could flow from FB1 to IG1 via a hard-link and then to IG2 via intra-app soft-matching. Alternatively, data could flow via soft-matching from IG2 to IG1, and then via a hard-link to FB1.

If intra-app SM and/or inter-app (M-M) SM occurs, we may see similar risks of identity leakage in our profile recommender systems, such as PYMK, AYMF, Groups, etc. in Future 3.

Commented [37]: To be precise, this scenario is possible today w/o future 3, right? Does Future 3 make this more or less likely?



II. **Improve or Rework Identity Sync** (Lack of user knowledge)

The Account Center in Future 3 will house users' various profiles with the option to tailor which profiles are synced to others. There will be one set of credentials across all of the Meta accounts' profiles, which they can also use to access third-party apps and bring their preferred profile and digital assets, such as NFTs, with them outside Meta platforms. Users will need to be savvy enough to manage their identities and content across VR and 2D sites as well as 1st party and 3rd party apps. Currently, no other social media site enables users such a broad range of interaction with their communities and content. Ensuring users gain this much needed know-how will require multi-pronged educational and transparency efforts.

Feedback from external stakeholders and users has demonstrated that Identity Sync is a confusing product that fails to give users granular control over which identities are synced and discoverable across apps. The difference between adding accounts to Account Center (enabling cross-app data use and combination), Connected Experiences, and ID syncing are not clearly explained to users. Product and XFN teams should work together to determine the best course of action: we may decide to (1) omit Identity Sync all together and give users granular discoverability controls, (2) allow users more granular controls within Identity Sync with better explanation and information about what ID Sync does, perhaps renaming and reconfiguring ID Sync all together.

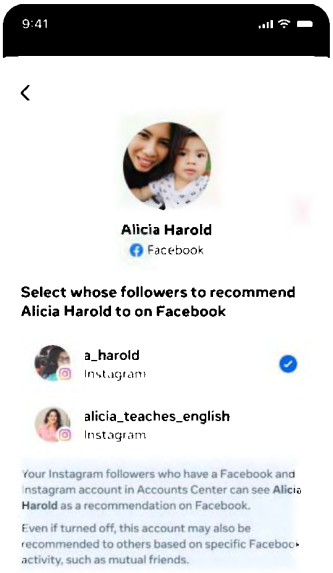
In addition to improving Identity Sync, clear internal[HYPERLINK "https://docs.google.com/document/d/1Rfw5flwzxxJ9IHJLI-P7WtMkYaLfhly0kADYOtcZwKc/edit?usp=sharing" \h] and user education about accounts and identities will be key to successfully landing Future 3 with users.

III. Create a cross-app discoverability control

While risks of identity leakage may increase with Future 3, there is also the opportunity to introduce new transparency and controls for users to achieve the unique cross-app experience they are seeking. For instance, we've already tested a control on Instagram that [HYPERLINK "https://docs.google.com/presentation/d/1FXvy_4Gka05XUIqxtRv9DiaXF_4dQ1DaTGVeD7tH__Y/edit" \l "slide=id.g1f9a6deb2a8_0_593" \h] users to decide whether or not they want to be tagged on Facebook. The FX Growth team has [HYPERLINK "https://docs.google.com/presentation/d/1c49EizZjEk4YpDRWh0QhaVIqdY3hzPs1jxX1AIGKrgo/edit" \l "slide=id.g144d14c5ce8_0_0" \h] a new Friending/ Following discoverability setting that would allow users to select which of their cross-app profiles they would like to be discoverable to others. While making firm commitments in cross-app settings in Future 3 will pose a challenge, there are opportunities to introduce more granular options for users, particularly in cross-app friending and following.

Commented [38]: Shouldn't this setting be symmetric? If the user wants profile A graph to be shared with profiles B, C, D… the inverse is probably true too?

Commented [39]: Why is this?



IV. Streamline and improve friending and following transparency and controls across apps

Currently, friending and following disclosures and controls vary across our Family of Apps. Users can choose to only be recommended to friends of friends on Facebook, but no parallel control exists on Instagram. On Horizon, users have packaged privacy options (packaged options that

allow them to control who follows them and whether their followers see their active status.) On Instagram, users can keep their profile private, while Facebook users cannot.

These differences in audience management, profile and post visibility, and discoverability across apps make controlling identities more difficult for users and increase accidental sharing of personal information. While some differences may be required due to the nature of each platform, we should have guiding principles for parallel friending and following controls across apps.

See the Friending and Following Policy Framework for unified F&F standards across current and future products. Future 3 F&F Guidance is currently being drafted, but some of the most important recommendations include:

- Set the friending/follower settings to the most privacy-protective by default. Prevent unintentional oversharing of personal information and/or unintentional discoverability.
- Allow users to manage who can search for specific profiles. Settings should be most privacy-protective by default (e.g. "Only Me" for "How Users Find You and Contact You" or "Who Can Look You Up" in FB).
- Unsynced profiles cannot access messaging threads in the other synced profiles in order to prevent unintentional messaging to friends not associated with a synced profile.
- Account Settings will be accessible only from the primary Meta account.
- While some settings may be managed at the Meta Account level, some privacy settings should be managed independently for each profile, allowing users to customize the level of privacy for each one. (In the F/F context, this may entail allowing users to individually manage to whom a profile can be recommended to.)
- When accessing individual profile friending/follower settings, a disclaimer should appear that tells the user they are only adjusting the F/F controls for an individual profile.
- When a profile blocks another profile, the blocked profile and other profiles owned by the blockee cannot mention or tag the blocker.
- When a profile blocks another profile, the blocked profile cannot message the blocker. The blocked profile's other profiles cannot proactively message the blocker, but can respond if the blocker initiates a message.

Commented [40]: What's the status quo across apps? I know FB starts with some permissive settings, but are IG/VR already more conservative?

Appendix: Soft-matching Deep Dive

Soft-matching and Friend/Follower Recommendations

What is soft-matching?

[HYPERLINK "https://docs.google.com/document/d/1CwxXZSrXLxKCyEtl_0wKvgYl8PVwvVyT5gjQqaLE1PI/edit" \h] for soft-matching is as follows: "Cross-account data use is considered soft matching where data is used to match the same user across two different Family of Apps accounts without user permission (either explicit or implied)." Because Meta is subject to a German Federal Cartel Office (FCO) order, we are deprecating **inter-app soft matching**.[2]

However, soft-matching *within the same app* (e.g. two IG accounts) is another kind of account matching that may also be occurring. Since our compliance efforts with the FCO are focused on inter-app soft matching (i.e. FB<>IG), we have not yet remediated **intra-app soft matching** (i.e. IG<>IG) to the same degree as inter-app soft matching. Furthermore, there is a possibility that intra-app soft matching *may result* in inter-app soft matching.[3]

How does soft-matching lead to identity leakage? (PYMK, AYMF)

Both inter-app soft matching and intra-app soft matching can lead to identity leakage – namely when we suggest accounts through features like FB's People You May Know and IG's Suggested Accounts (a.k.a. Accounts You May Follow, AYMF). Before inter-app softmatching was deprecated, a user's FB or IG profile may be a top recommendation to the other profile's friends or followers. For example, if a user has a Facebook account, "FB1" which represents their 9-to-5 persona, and an Instagram account, "IG1" for their gamer persona, the FB1 profile might surface as a PYMK recommendation to IG1 followers also on Facebook; conversely, the IG1 gamer profile may surface as a AYMF recommendation to FB1's friends on Instagram.

Likewise, intra-app soft matching may lead to identity leakage. For example, if IG1 and IG2 are soft matched. There is a possibility that IG2 is going to be the top recommendation in IG's AYMF (Accounts you may follow) to IG1 followers.

Can soft-matching lead to identity leakage outside of friending and following? (GYSJ, etc.)

Possibly. While more in-depth technical research needs to be conducted, it's possible identity leakage and soft-matching presents a risk *in other features* where we suggest users' accounts based on personalization. Like PYMK and AYMF, Search and Photo Tagging suggest user

---

[2] Meta faces continued scrutiny from privacy and competition regulators regarding the use of user data across the family of apps. For example, Meta is subject to enforcement by the German Federal Cartel Office (FCO) and has received enquiries from the Irish Data Protection Agency (IDPC) regarding the use of cross-account data.

[3] For example, if AC1 contains FB1 and IG1 and AC2 contains IG2. If IG1 and IG2 are soft matched, there is a possibility that FB1 is also soft matched with IG1. We do not know if intra-app soft matching actually leads to this kind of inter-app soft matching, but it is a theoretical risk.

accounts based on a number of data inputs, personalized for each user. FB's Groups You Should Join and Events also appear as recommendations to users; while they do not recommend users to friend/follow per se, they may still lead to identity leakage when they recommend groups/ events and contain member details.

What about accounts added to the same Account Center?

Note that our current system of cross-account data usage via Account Center gives users the ability to opt-into a "hard matched" account experience. Since 2020, users have had the option to add their [HYPERLINK "https://about.fb.com/news/2020/09/privacy-matters-accounts-center/" \h]; when users choose this experience, we give them [HYPERLINK "https://docs.google.com/presentation/d/1LFWEc1R_6VXhi2u6NgROIhTQzHVht-xHeCEAi8LI2KA/edit" \l "slide=id.g206c5d0720d_1_7" \h] – including the fact that we "combine and use your info across accounts [to] suggest friends and accounts to follow." In the mitigations section, we discuss additional identity leakage protections users have access to through Account Center.

META3047MDL-146-00072943

Metadata

All Custodians	Meta Platforms	SEMANTIC
All Paths	/Meta Platforms	SEMANTIC
Confidentiality	HIGHLY CONFIDENTIAL (COMPETITOR)	SEMANTIC
Primary Date	04/27/2023	DOC_TYPE_ALIAS