Opportunities and Challenges for Standardization in Mobile Social Networks

Laurent-Walter Goix, Telecom Italia

laurentwalter.goix@telecomitalia.it

Bryan Sullivan, AT&T

blsaws@hotmail.com

Abstract

This paper describes the opportunities and challenges related to the standardization of interoperable "Mobile Social Networks". Challenges addressed include the effect of social networks on resource usage, the need for social network federation, and the needs for a standards context. The concept of Mobile Federated Social Networks as defined in the OMA SNEW specification is introduced as an approach to some of these challenges. Further specific needs and opportunities in standards and developer support for mobile social apps are described, including potentially further work in support of regulatory requirements. Finally, we conclude that a common standard is needed for making mobile social networks interoperable, while addressing privacy concerns from users & institutions as well as the differentiations of service providers.

1 INTRODUCTION

Online Social Networks (OSN) are dominated by Walled Gardens that have attracted users by offering new paradigms of communication / content exchange that better fit their modern lifestyle.

Issues are emerging related to data ownership, privacy and identity management and some institutions such as the European Commission have started to provide measures for controlling this.

The impressive access to OSN from ever smarter mobile devices, as well as the growth of mobile-specific SN services (e.g. WhatsApp) have further stimulated the mobile industry that is already starving for new attractive services (RCS[1]). In this context OMA[2] as mobile industry forum has recently promoted the SNEW specifications that can leverage network services such as user identity and native interoperability of mobile networks (the approach promoted by "federated social networks").

Besides the business opportunities behind this concept, technical issues must be addressed re social network protocols support for deployment, security and scalability needs in a distributed context, and especially considering user concerns around privacy.

1.1 Problem Statement

OSN have overcome the limits of synchronous real-time communication by introducing the interactive user's wall. This new feature was probably one of Facebook's key success factors, since Facebook was the first to introduce this feature in 2006 [1].

This wall-based approach has contributed strongly to the growth of mobile social network applications, which have further contributed a tremendous boost to data usage in the telecom

1 http://www.gsma.com/rcs/

2 http://www.openmobilealliance.org/

industry over the last years, through the massive adoption of smartphones and the explosion of broadband and mobile internet accesses worldwide. Managing this data usage explosion has become a key priority for the telecom industry as current "mobile" access to OSNs lack of mobile network-friendly characteristics, in particular for notification support and for handling network connectivity changes

In addition, as the number of users grows, concerns about privacy and data ownership increase consequently. This has raised significant concerns at institution level such as the European Commission, which has created a self-regulatory agreement - signed by major OSNs active in Europe - that fixed the principles that an OSN should respect to operate in EU countries.

1.2 Federation of Distributed Social Networks

A branch of the Social Web community seems to go in the direction of a distributed architecture, which can potentially scale better and in which data can be controlled more easily in terms of persistence and ownership. In 2010 the OStatus specification[3] pioneered in that direction of "federation of social networks" as a suite of protocols allowing people standing on different OSNs to communicate with each other, with each of these protocols standardizing a specific part of the overall communication process. However, success was not as big as expected namely because of little interest from current major OSNs that are not yet interested in federating with each other, and yet a de-facto or promoted standard has to come. An interesting trend may come from enterprise social networks that could find value in opening their own network to their partners just as for emails and therefore need a standard specification to interoperate.

1.3 Mobile Federated Social Networks

Long before the Social Web era over the Internet, mobile (communication) networks have been (and still are) the first global – worldwide – communication network to interconnect people, for real-time and near real-time communications across telecom networks, with user phone numbers as the key user identity.

The OSN "wall-intermediated" communication paradigm became of interest to the OMA in 2010, as its members considered the ability to leverage network assets and related proposals for a standard solution that could integrate with current (and planned) mobile network services. A first analysis revealed that current "mobile" access to OSNs suffers from incomplete support for some specific aspects of the mobile service environment:

- the frequent usage of HTTP polling instead of push notifications for near real-time status updates,
- where push notifications are used, maintenance of discrete long-lived HTTP connections for this as compared to using shared-bearer notification systems,
- lack of support for mobile identity/authentication ("Over-The-Top"),
- a limited user experience in case of loss of connectivity or roaming, due to lack of support for deferred delivery of posts/messages,
- no integration with SMS/MMS or other existing mobile communications service enablers.

3 http://www.w3.org/community/ostatus/

Consequently, the SNeW (Social Network Web) [2] specification work started, targeting these gaps with an end-to-end vision for mobile users and interoperability with existing network services.

The following advantages have been identified for mobile federated social networks towards end-users:

1. The "social" – asynchronous – (tele)communication paradigm can be easily integrated with current real-time communications services.
2. Mobile networks subscribers already have, and actively use, a globally unique user identity (their phone number)
3. Mobile networks are natively interoperable to reach users worldwide no matter their operator
4. Mobile network operators provide a high degree of trust in terms of privacy of communications [3]
5. Mobile networks have assets that can improve the user experience (e.g. seamless login through network-based identification, real-time push notification, etc)

Technically, the current OMA SNEW specifications have been addressing mobile federated social networks in the following way:

- Reuse of existing, and in particular the most popular open specifications from the social web industry in terms of protocols and data models, applying necessary "profiling" wherever needed, also based on the explicit requirements from the mobile industry. This includes ActivityStreams[4], OpenSocial Social API specifications[5], OStatus (PubSubHubbub[6] & Salmon[7]), OAuth2, Host-Meta, WebFinger and OExchange.
- Reuse of existing standardized network technologies and services provided by Mobile Network Operators (MNOs), in particular for identifying (and authenticating) users, routing data across operators and integrating with existing communication services.
- "Regulatory-friendly", trying to provide early technical solutions that address in particular the EC concerns (& principles) in terms of i) "privacy by default", ii) data portability and iii) "right to be forgotten"

Technically, the combination of web-based standards together with existing network services provided simple solutions for a variety of features, such as i) autoprovisioning of the mobile client, ii) routing of social communications across operators, iii) phone contacts discovery. For example, network-based authentication can simplify the authentication procedure in OAuth flows, and the resolution of the target SNEW Server of a user benefits from existing phone number resolution and

4 http://activitystrea.ms/

5 http://opensocial-resources.googlecode.com/svn/spec/2.5/Social-API-Server.xml

6 https://code.google.com/p/pubsubhubbub/

7 http://www.salmon-protocol.org/

routing procedures across MNOs (like it happens already for MMS or RCS routing), which can then make extensive use of web discovery procedures to find the most appropriate endpoint.

2 STANDARDIZATION OPPORTUNITY IN THE MOBILE SOCIAL ENVIRONMENT

By developing a reference implementation prototype in parallel with the active participation in standardization activities, we could pinpoint caveats in terms of features, performance and privacy from the currently available specifications.

The uptake of mobile federated social networks by MNOs surely depends on agreements at national or international level as well as sustainable business models with respect to partnering with OSNs, but is also strongly related to the maturity of technologies and standards that the Social Web community will define and promote. Technology-wise, improvements can be made in standards of the mobile and web industries to improve core social web specifications, as well as to enable more mobile- and privacy-friendly solutions, or by defining guidelines and best practises for mobile clients to optimize network usage and scalability across providers.

2.1 Device Contacts discovery

In a distributed context, discovering user capabilities of your contacts is of great importance. RCS has defined this feature and so did SNEW, without needing to upload the user's full address book at once. However standards would be needed to optimize such discovery procedure in a distributed fashion, while ensuring user privacy and privacy of the user's contacts.

2.2 Real-world interactions

Interesting use cases of the content-type "application/stream+json"[8] dedicated to the Activity Streams data model can be found on mobile devices, and would benefit from standardization to simplify user experience. In particular this can result in "templates" of social activities that can easily be embedded, or indirectly referenced through a URI, into real-world markers such as NFC tags, 2D barcodes (e.g. QR codes), Augmented Reality active targets and the like.

Such technology, if widely deployed as standard, could easily be employed in a number of real use cases leveraging any OSN. For example, a user could scan a QR code on an advertisement with her phone to automatically preload a "like" of that offer on her mobile client, ready to be shared with her friends. Similarly, she could easily check-in at a concert venue by tapping the event poster at the entrance gate with her NFC-enabled phone.

2.3 Security & privacy

While the OAuth framework provides a useful foundation for user authorization, e.g. as used in OpenId Connect, the user experience for this on mobile devices still suffers from dependency upon interstitial dialogs and manual credentials entry. Since many users already access-control their devices using screen lock passwords or PINs, the ability to leverage network-based authentication in OSNs can provide a more seamless SSO experience. Even in roaming scenarios, the ability to leverage the world-wide-interoperable and highly trusted system of user identification inherent in mobile networks can significantly simplify the user experience, while providing strong multi-factor identity assurance. Whether this ability depends upon any specific standardization efforts is TBD,

8 http://tools.ietf.org/html/draft-snell-activity-streams-type-01 (Work in progress)

but should be considered in discussions about the intersection of identity/authorization and social network applications.

2.4 Resource usage

Both data usage and battery life can significantly affect the user experience of OSN apps. While the need to manage resource utilization more effectively can be partially addressed by better app development techniques (e.g. per the GSMA Smarter Apps Guidelines[9]) and tools (such as AT&T's free/open-source Application Resource Optimizer (ARO)[10]), standards are needed to enable fundamental capabilities promoting more resource-efficient designs. These include the following:

- Methods of integrating connectionless or shared-connection notification systems into web-based OSN apps, e.g. via the W3C Push API[11] in development. This API can provide a simple method for apps to stay connected for event delivery, without having to maintain a discrete long-lived HTTP connection. Once supported by browsers, integrating the Push API into the signalling-network based push systems currently operated by MNOs (e.g. SMS and OMA Push[12]) will provide the most effective use of network and device resources, while enabling always-connected OSN apps across MNOs.
- Similarly for native apps, subscription to SN information could be easily adopted, e.g. by leveraging PubSubHubbub-like subscriptions to SSE (no HTTP callback channel usually available on the device) to negotiate further connectionless notification-channel(s) by exchanging Push capabilities through dedicated HTTP headers, like it was proposed in OMA SNEW.
- Methods of enabling OSN apps to express compatibility with deferred XHR request processing, which can be used by the device platform to optimize Radio Resource Control[13] e.g. by holding requests until another app establishes a data connection. This new XHR feature could be exposed by adding a "max-delay" attribute (e.g. in seconds) to the XHR API. Use of this new feature can also obviate privacy concerns with exposing network state to web apps, for the purpose of app-layer deferred request processing e.g. through JavaScript. Meeting the same objective (network-state-aware processing) as a *service* can provide equivalent or better benefits, without concerns over exposing current connection type/status to apps, and could be provided to apps without any need for user awareness or opt-in.
- Methods of enabling OSN apps to express compatibility with shared request processing, which can be used by the device platform to minimize the number of discrete TCP connections over which requests are handled. This new feature could be exposed by adding a "shared-ok" attribute (boolean, default *false*) to APIs over which it could be used (e.g. XHR and EventSource). When *true*, the device could use a shared connection (e.g. a Websocket maintained for this purpose) to tunnel the related requests to a network proxy/gateway, where the requests are extended to the origin server. Use of this capability

9 http://smarterappsguidelines.gsma.com/

10 http://developer.att.com/developer/legalAgreementPage.jsp?passedItemId=9700312

11 http://www.w3.org/TR/push-api/

12 http://technical.openmobilealliance.org/Technical/release_program/push_v2_3.aspx

13 http://www.youtube.com/watch?v=4baYdgBBgFs

could significantly reduce the number of discrete over-the-air TCP connections, which especially for long-lived connections can have a significant effect upon resource utilization.

On the server-to-server side, PubSubhubbub and Salmon have yet to be analysed in terms of content distribution load amongst providers, typically leveraging unicast notifications on a per-user basis that could easily generate huge amount of traffic amongst large OSN providers, and would benefit from optimization techniques such as the ones studied for event notifications in the IMS infrastructure.

2.5 Regulatory Challenges

The European Commission has defined a set of principles [4] for SNS that target EU citizens as their customers, subject to self-regulation, i.e. for SNS to submit a self-declaration form explaining how they address these principles in their SNS. Assessments are performed periodically to monitor the implementation of these principles.

Some of those principles relate to features that may not be impacted by standards, but many other do, e.g. to protect users from being searchable unless they give explicit consent, restrict default privacy of user information (with further restrictions re access to sensitive data). The "right to be forgotten" (hence requiring the user's OSN to delete her information upon account deletion) and "data portability" principles advocated by the EC [5] surely require major attention and standard specification work over a federated network rather than on a single walled garden. In that sense OMA SNEW has analyzed such principles and attempted to address (some of) them although future work is needed (and welcome) to achieve a truly regulatory-friendly standard.

3 CONCLUSIONS

Mobile social networks have become mainstream due to the concurrent explosion of OSNs and smartphones. However, current popular mobile solutions are walled gardens, delivered by over-the-top players that do not leverage network services in ways that could benefit user experience, accessibility, trust, and resource efficiency. In this paper we examine the recent evolution of the social web standardization landscape, in particular from the mobile industry, and the open challenges that standards-setting organizations and similar bodies need to meet to foster the deployment of "mobile federated social networks". We would warmly welcome those initiatives to join forces into a common standard for making OSN interoperable, while addressing privacy concerns from users & institutions.

4 REFERENCES

[1] Marshall, M. Facebook launches "News Feed" and "Mini Feed" – As YouTube invades turf. venturebeat.com, September, 2006. http://venturebeat.com/2006/09/05/facebook-launches-news-feed-and-mini-feed-as-youtube-invades-turf/

[2] Open Mobile Alliance, "Social Network Web Enabler 1.0 draft", Jun 2013, http://member.openmobilealliance.org/ftp/Public_documents/CD/Permanent_documents/OMA-ER-SNeW-V1_0-20130603-D.zip

[3] Ernst & Young, "The top 10 business risks in telecommunications", 2012. http://www.ey.com/GL/en/Industries/Telecommunications/Top-10-risks-in-telecommunications-2012

[4] "Safer Social Networking Principles for the EU", European Commission, February 2009. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

[5] "How will the data protection reform affect social networks?", European Commission, 2012. http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf