Ditch Social Login for Mobile Login, $20 Billion Opportunity for Network Operators

Operators have a golden opportunity to capture share of the $20 billion digital identity market, but it requires adoption of the GSMA Mobile Connect technology

ESPOO, FINLAND, August 29, 2018 /EINPresswire.com/ -- A massive privacy breach occurred in April 2018 when Cambridge Analytica obtained information belonging to 87 million people because users unwittingly allowed Facebook to share their own and friends' data with a personality test app.

Cambridge Analytica was roasted by the media. But there is a less reported side to data sharing when companies – retailers, travel sites, banks, media and a plethora of apps – invite people to take the oh-so-simple and hassle-free step of logging into their application or service using a social media account.

The reason people use social login provided by companies such as LinkedIn, Google, Twitter and Facebook is convenience. Site developers use it for its low friction signup process. Rather than requiring users to create yet another user name and password for their site, developers can simply piggyback on social media giants' generosity for smooth authentication.

Joakim Nylund, CEO Exomi

If a retailer like Safeway uses social login, it is not only using those social media companies to authenticate users, it is also giving user data to those companies – and their partners. The retailer on the other hand gets access to the data, which users - and their friends - have on Facebook. Of course users have given their consent for that by accepting the default social login terms and condition (everybody knows the small print, which nobody reads).

> **"** Providing consumers with Mobile Identity and an easy and safe digital identification procedure will provide network operators the perfect gateway to a plethora of new business opportunities."
> *Joakim Nylund, CEO Exomi*

But this is not what a consumer or a retailer would choose if they had a safer login process.

After the Cambridge Analytica scandal, Facebook assured users and governments that it is going to limit how much data its partners get. It's not clear how Facebook actually plans to do this, because, let's not forget, it is collecting data, segmenting people and monetizing the results to pay wages and keep shareholders happy. But, can the damage on social login be fully repaired anymore?

If there was a Mobile Login button next to the social login buttons on websites, the answer is a resounding YES!

Mobile Login

Frequent privacy scandals have already educated the general public enough about the importance of digital privacy. The time is now ripe for change when it comes to consumer expectations and one that presents a golden opportunity for the mobile operator community.

There is a global standardized technology already in place and defined by the GSMA, Mobile Connect. According to the GSMA, the Mobile Connect service has already been adopted by more than 50 operators, Deutsche Telekom and SK Telecom among others, in approximately 30 countries worldwide and the mobile identity service is thereby available to 300 million subscribers.

Mobile Connect is the mobile operator-facilitated secure universal identity solution. By leveraging the high level of security inherent in mobile networks and operators' knowledge of their users' identities, it enables consumers to register and login to websites and apps in a safer way. It also allows users to authorize transactions whilst sharing only data needed to verify the attributes to complete that transaction.

Mobile Connect features an inbuilt global roaming capability, which means that websites and app and service developers only integrate with one operator to get Mobile Login for all users accessing their service. For end users, Mobile Login works anywhere in the world given that they have accepted the general Mobile Connect terms with their operator.

Mobile Connect authentication and authorization events produce so called security tokens that integrate the user's identity, permissions granted, validity time and other attributes. The use of tokens makes these events more secure, traceable and valuable compared to the traditional method of transmitting MSISDNs (phone numbers) to all services that require user identity. Operators can also utilize security tokens to control access to resources such as SMS delivery, billing and carrier APIs to a high level of detail and trace transactions back to the user's specific consent and device.

Mobile operators are regulated by national communication service authorities and thus considered as more privacy-abiding and trusted digital identification providers compared to social networks. In GSMA's Mobile Connect, users are requested for consent to allow data sharing for each individual service and app for maximum transparency.

20 Billion Dollar Opportunity for Mobile Operators

The momentum for a mobile operator login service has been built. McKinsey estimated the current market (Q2/2018) for identity verification services at around $10 billion, and forecasts it will reach $20 billion by 2022.

The main benefit operators see in digital identity is not only about the transactions carried out through their networks. It is the massive incremental brand value and tight, trust-based, long-term liaison with customers that they can build by taking the role of digital identification provider.

For many people, the digital world can be frightening, yet an increasingly important place in everyday life. Cyber-security becomes part of daily life and that's not easy for all. Mobile service providers have always had the image of a being a trusted partner and Mobile Connect is a perfect platform to build upon that reputation.

Mobile Login Has Come of Age

Looking ahead, there is little doubt that the ability to provide consumers with Mobile Identity and an easy and safe digital identification procedure will provide network operators the perfect gateway to a plethora of new business opportunities.

The time to move ahead is now before the next data scandal makes the front page.

Exomi is showcasing its mobile solutions at the Mobile World Congress Americas in Los Angeles in September 12-14th at the Finland Pavilion (Stand 1360). Other telecom, video, cybersecurity and IoT companies showcasing at the Finland Pavilion are Bcaster, Cloudstreet, Convergentia, Creanord, F-Secure, Kaitotek, Sitowise and Tosibox.

Finland Pavilion is organized and funded by Business Finland's Connectivity from Finland business acceleration program. Business Finland is fully-owned by the Finnish Government.

Ends

Hugh Paterson
Whoosh PR
+447768175452
email us here

This press release can be viewed online at: http://www.einpresswire.com