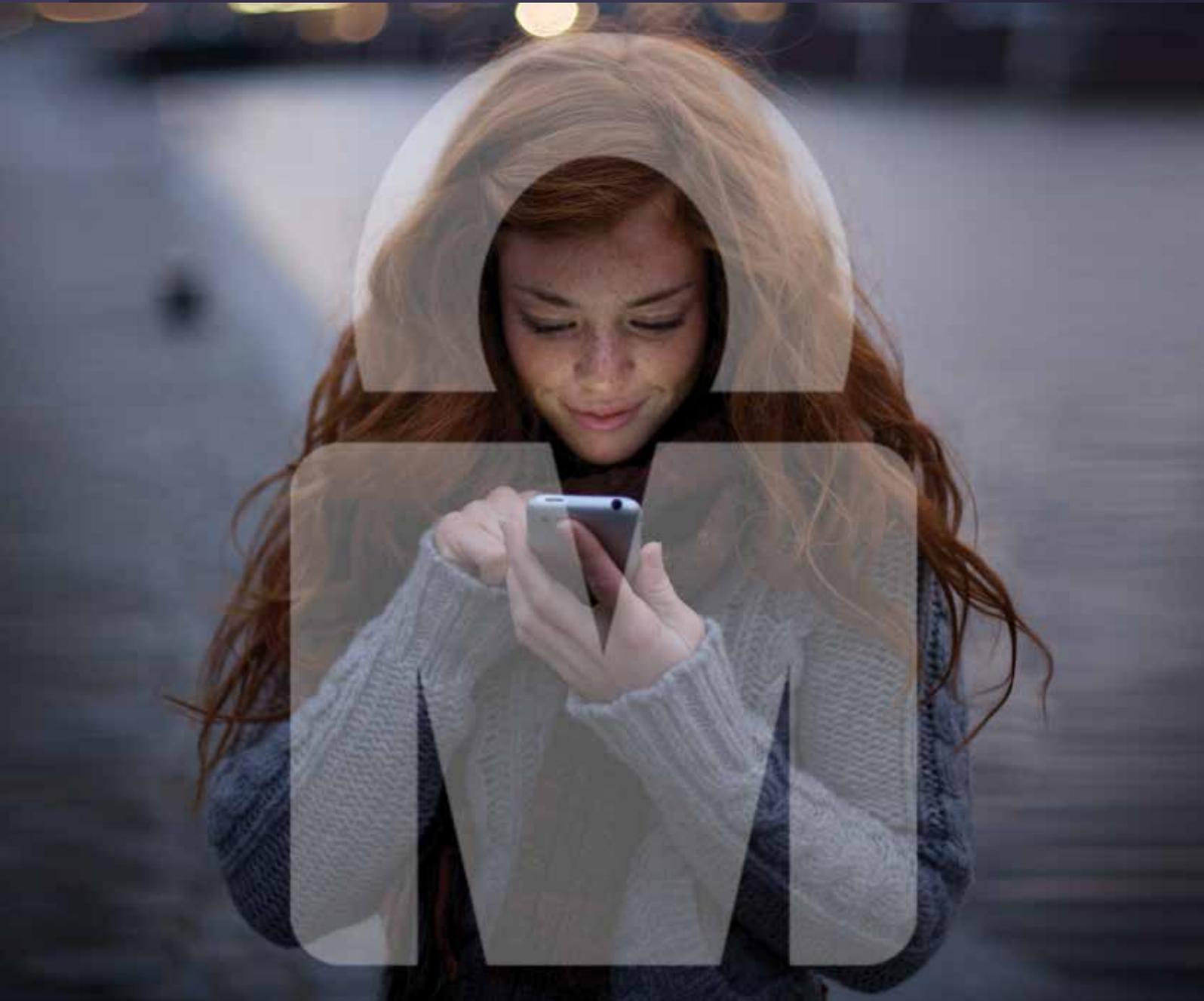




Secure digital identity is now in our hands

MOBILE CONNECT CONSUMER RESEARCH REPORT: UNITED STATES





As the digital economy expands, individuals, businesses and governments are looking for ways to interact easily online without compromising security and privacy. The GSMA Personal Data programme aims to help digital service providers and consumers find the optimum balance between privacy, security and convenience.

The programme and its operator partners have prioritised the development of digital identity services. Working together, they aim to bring to market digital identity solutions that provide a safe, seamless and convenient consumer experience, a consistent user interface and low barriers to entry across the digital identity ecosystem.

The GSMA and its mobile operator members are leading the development of 'Mobile Connect', a service for secure authentication and identification that helps address the current trade-off between security and ease-of-use.

gsma.com/personaldata



To gain insights into consumers' evolving attitudes to mobile and digital services, the GSMA commissioned KRC Research to canvas the views of smartphone users in the US about their attitudes towards online authentication and identification as well as the sharing of personal data. One of the main objectives was to better understand how consumers will respond to Mobile Connect. Conducted in February 2015, the study combined an online survey of 1,000 smartphone users and two focus groups in Chicago for face-to-face discussions.

The GSMA also commissioned Futuresight to ascertain online businesses and service providers' perspectives on authentication, identification and Mobile Connect. Between March and May 2015, Futuresight conducted 50 qualitative telephone and in-person interviews with service providers, including 17 government agencies and banks, in the US, UK, Germany, Singapore, Malaysia and India.

This paper, which summarises the key findings of these two pieces of research, is written primarily for governments and banks that could benefit from adopting Mobile Connect.

Contents

Executive summary	3
1. Digital challenges facing consumers and service providers	5
2. What do consumers want?	10
3. Introducing Mobile Connect	11
4. Example use cases	15
5. Conclusions	17

Executive Summary

Americans are becoming increasingly reliant on the digital services offered by online retailers, content providers, government agencies and banks. Yet sharing information with these service providers can be a frustrating and unsettling experience. Most US consumers struggle with log-in mechanisms that require them to remember multiple usernames and passwords, while worrying about the privacy implications of sharing personal data online.

Both consumers and service providers are looking for easier and more secure ways to share information. Mobile Connect was perceived by respondents as addressing this demand, according to the findings of the GSMA's research. In particular, service providers are interested in Mobile Connect's potential to:

- **Accelerate and ease verification and authentication to make it easier to interact with consumers.**
- **Reduce friction (e.g. dropped logins, abandoned shopping carts) to increase registration and engagement.**
- **Enable access to subscriber attributes (regardless of their operator) to provide better and more secure services.**

Online retailers, content companies, banks and government agencies all see benefits from adopting Mobile Connect, the research found. In these sectors, there is a clear need for better verification mechanisms to support the smooth and secure exchange of sensitive personal data.

For example, retailers, banks and government agencies are interested in using Mobile Connect to determine an individual's location for a variety of purposes. Location is one of several attributes that can be verified by Mobile Connect and then used by retailers to enable the personalisation of communications and services, thereby increasing customer acquisition, engagement and retention. In the case of banks and government agencies, location and other attributes can be checked via Mobile Connect to verify service entitlement and help counter fraud.

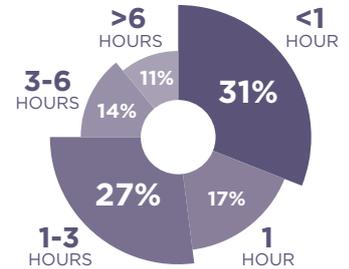
Consumers in the US also see advantages in adopting Mobile Connect: 71% of respondents said they would be likely to adopt Mobile Connect as their primary log-in for most websites, apps and online services. Almost 90% of the 1,000 smartphone users interviewed were attracted to Mobile Connect's three key propositions:

- **Universal log-in for multiple websites**
- **Strong security**
- **Control over personal data**

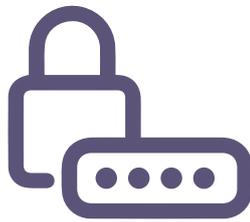
The research suggests that the widespread deployment of Mobile Connect by service providers could oil the wheels of digital commerce, by providing a simple and convenient means of managing permissions for sharing and verifying personal attributes, such as location, age and shopping needs.

CURRENT CHALLENGES FOR DIGITAL SERVICES

Americans are becoming increasingly reliant on the digital services offered by online retailers, content providers, government agencies and banks. Yet sharing information with these service providers can be a frustrating and unsettling experience. Most US consumers struggle with log-in mechanisms that require them to remember multiple usernames and passwords, while worrying about the privacy implications of sharing personal data online.



However, as consumers become more reliant on digital services, frustration around access and privacy grows.



87% ARE CONCERNED ABOUT

“the security of my identity and data when using the internet.”

WHO DO THEY TRUST WITH THEIR DATA?

Consumers feel their data is very or somewhat secure with the following organisations:



88% MY BANK



82% MY INSURANCE PROVIDER



73% MY MOBILE OPERATOR

Mobile Operators over Internet players are optimally positioned as providers of secure digital identities.

INTRODUCING:



Mobile Connect Log-in

Mobile Connect is the operator-led secure authentication service.



71%

would be likely to use Mobile Connect as their primary log-in for websites and apps



SECURE

84% feel Mobile Connect provides **stronger security** than current log-in due to the combination of phone and PIN



PRIVATE

87% liked that Mobile Connect provides **anonymous log-in** for services
86% found the **privacy principles**, governing all that adhere to Mobile Connect appealing too.



CONVENIENT

85% agreed that Mobile Connect enabled **easy log-in** using your phone and PIN.

Suggested services to use Mobile Connect included:



More secure financial transactions



Universal log-in banishing multiple passwords



Parental Control



Pre-identification for call centres



More secure online banking



and more

1. Digital challenges facing consumers and service providers

Growing demand for and reliance on digital services

In the US, over three quarters of consumers now own a smartphone¹ and are becoming increasingly reliant on their handset to access a wide range of digital services. One quarter of smartphone users in the US spend at least three hours a day accessing the Internet from their handsets, according to the GSMA's research.

Over time, US consumers expect their handsets to take on an even more central role in their lives. Within five years, approximately half of the respondents in the online survey said they expect to be using their mobile phone to perform daily tasks, such as making payments, and storing loyalty cards and coupons (see Table 1).



TABLE 1: WHAT DOCUMENTS OR PROCESSES DO YOU EXPECT TO STORE, OR CARRY OUT, USING YOUR MOBILE PHONE BY 2020?

Making a payment to an online store without cards	50%
Storing loyalty cards and coupons	48%
Tickets for travelling on public transport	35%
Registering or sharing information with your doctor	35%
Actively protecting yourself, your home and family from hacking and fraud	33%
Authorising access to home internet and TV	33%
Storing your driving license	28%
Proving your age when purchasing alcohol or cigarettes at a self-service check out	24%
Filing your tax returns	23%
Voting in elections	22%
Entering your place of work, VPN, printers etc.	19%
Entering a country using a passport	17%

At the same time, retailers, content companies, banks, governments and other online service providers are increasingly adopting "mobile-first design"- prioritising the mobile user experience on handsets- for their digital services, according to interviews commissioned by the GSMA. Service providers, particularly those in the US and other developed countries, reported growing demand from end-users to log-in and transact via mobile.

Individuals’ challenges and concerns

But even as consumers become increasingly reliant on their mobile phones and digital services, most are dissatisfied with the process required to access these services and their lack of control over their data and privacy.

The GSMA’s consumer research found that many people in the US struggle to complete the log-in process employed by websites and apps; 15% of US smartphone users said they encounter problems logging into online services on a daily basis, while more than one third (36%) have problems on a weekly basis and 59% on a monthly basis.

Most consumers in the US also worry about the privacy implications of the increasingly digital and data-driven economy. In the consumer study, 62% of the respondents agreed with the following statement: “Online privacy and security is a major concern of mine and I do everything I can to make sure I’m protected.”

Many digital services rely on consumers sharing some information about themselves and most individuals accept that trade-off: 63% of the respondents in the US said they are “ok letting companies know a little about me in exchange for access to services or products.” However, individuals are more comfortable sharing some types of data than others. Although 78% are comfortable sharing data about their shopping and purchasing needs in exchange for deals and other benefits, only 51% felt the same about sharing details of their device, such as the reference numbers of their handset, operator account and SIM card (see Table 2).

59% STATED THEY:

“Had problems logging into online services on a monthly basis.”

TABLE 2: % COMFORTABLE SHARING DATA ABOUT THEIR:

Shopping & purchasing needs	78%
Personal interests and preferences	72%
Websites visited	72%
Electricity, gas and water bill/usage data	71%
Personal data: name and address, mobile number, email address, dob	60%
Phone account data: contract type, payment history	54%
Network data: operator’s name, phone location, roaming country	53%
Device details: technical details and reference numbers of your handset, operator account, and SIM card	51%

....in exchange for deals and other benefits

Service providers' challenges

Meeting consumers' desire to interact through the mobile channel isn't easy for service providers. They report that the small form factor of handsets and other user-experience constraints are holding back engagement and registration – an issue frequently referred to as “friction” in the interviews commissioned by the GSMA. In the case of high value transactions, the need for strong security further increases the friction involved, sometimes resulting in consumers abandoning the process.

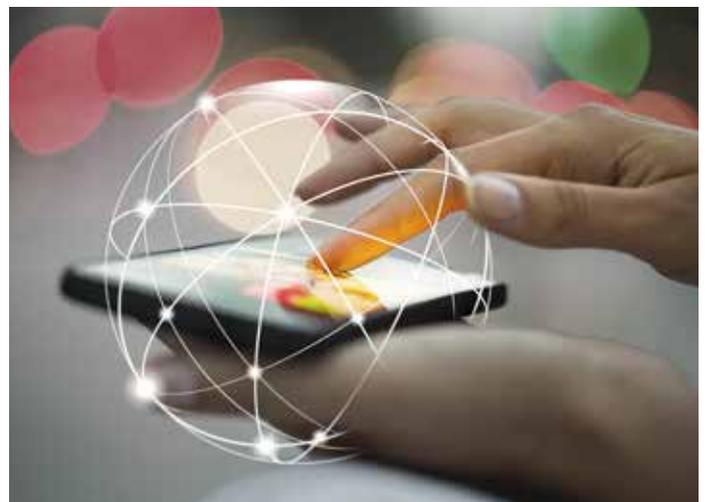
One US online retailer noted: “We know mobile is important to us, and we could do things much better; the current log in on mobile isn't a great experience, and we are definitely not converting browsers to purchasers on mobile at all well.”

“We know mobile is important to us, and we could do things much better; the current log in on mobile isn't a great experience, and we are definitely not converting browsers to purchasers on mobile at all well.”

US Online Retailer

For online retailers, another key challenge is to obtain and verify information about their customers and potential customers that can then be used to send tailored communications and offers. Some online retailers are reluctant to use social log in services in this context because they want to have a direct relationship with the user.

As consumers can switch between services so easily online, service providers acknowledge that gaining explicit consent to use their personal data is important to protect their reputation and maintain consumers' trust. Overall, service providers say that respect for privacy and maintaining a good user experience is increasingly important. However, service providers in developed markets report difficulty in gaining end user consent to use personally identifiable data for marketing and profiling purposes.





In some contexts, requests for explicit consent can be problematic and even counterproductive. Banks and governments, in particular, say they need implicit consent to use an individual's personal data for various purposes, such as fraud reduction, the exchange of credit-scoring information between banks and government security, planning and resourcing.

To strike the right balance between obtaining transparency and irritating end users with repeated consent requests, many service providers are looking for a way to obtain explicit 'one-time' consent, coupled with an explicit and transparent method of 'opting out'. Ironically, some service providers believe consumers are less likely to opt-out if they think it is easy and simple to do so.



2. What do consumers want?

Greater convenience

Among consumers in the US, there is a strong desire for a more convenient means of logging in securely to online services. Almost nine out of ten (89%) of the respondents in the consumer survey in the US would welcome a single log-in solution - a username and password that they were confident were secure - for all or most websites. More than half (57%) said such a solution would be “very beneficial”.

87% STATED THEY ARE:

“Concerned about the security of my identity and data when using the internet.”

Greater control

If individuals feel like they are in control, they are more likely to interact online and share relevant personal data. More than three-quarters (76%) of the respondents in the consumer survey said they would be likely to share information on their shopping and purchasing needs if they could control what data was shared with which advertiser, to make the ads they see online more relevant to them. Moreover, 70% said they would be likely to share information on personal interests and preferences on the same basis.

Greater security

Focus groups in the US were clear that greater convenience online and better control of their data had to be balanced with an improvement in security over their current login systems and habits. In the research survey, as many as 87% of Americans say they're concerned about security when shopping online or using the internet. Consumers in the US want a balance between convenience, control or 'ownership' of their own personal data, and a solution that keeps their data and identity secure.

3. Introducing Mobile Connect

Developed by the GSMA with a lead group of mobile operators, Mobile Connect is a secure authentication and identification solution. It provides:

- **Simple, secure access which leverages the inherent security of network assets via the individual's mobile phone for authentication.**
- **Support for anonymous log-in with control over what personal information is shared.**
- **An alternative to multiple passwords and access mechanisms, which can consistently be used at different security levels.**

A cross-operator solution, Mobile Connect uses an API Exchange to identify an individual's mobile network and utilises the handset ('something you have) and a password ('something you know') for two-factor authentication. The solution also supports other levels of authentication, ranging from 'seamless login' to very high security authentication using the SIM/Applet and PKI technology.



By accessing a global footprint through the API Exchange, Mobile Connect offers operators and service providers the benefits of scale, such as reach and availability.



71%

would be likely to use Mobile Connect as their primary log-in for websites and apps

Service providers' initial response to Mobile Connect

The majority of service providers interviewed in the GSMA study were very receptive to the Mobile Connect concept. In particular, service providers were interested in Mobile Connect's potential to:

- **Accelerate and ease verification and authentication to make it easier to interact with consumers.**
- **Reduce friction (e.g. dropped logins, abandoned shopping carts) to increase registration and engagement.**
- **Enable access to services that utilise subscribers' attributes (regardless of their operator) to provide better and more secure services.**

The service providers welcomed Mobile Connect's potential to reach all of their customers across national boundaries and jurisdictions rather than just a subset. Once Mobile Connect has identified which mobile operator the consumer subscribes to, the service provider can use the mobile operator's authentication and attribute services that could, for example, confirm which country the user is in and what age band they belong to (see section 4 for more on potential use cases). Service providers were also very positive about the solution's ability to support authentication, identification and consent for sharing personal attributes across any platform or device.

The research suggests there is likely to be particularly strong demand for Mobile Connect from online retailers, content companies, banks and government agencies. In these sectors, which generally face the biggest challenges in terms of identification and friction, there is a clear need for better verification mechanisms. Facing intense competition, retailers are particularly interested in Mobile Connect's potential to support customer acquisition, engagement and retention through the personalisation of communications and services.

One US retailer commented: "Yes, this looks interesting. We are looking into how we can make the mobile experience better and this looks like something we could take on. Certainly username and passwords aren't the best way on a mobile device, so from a sign-on perspective, it's interesting."

Individuals’ initial response to Mobile Connect

Mobile Connect also resonates with consumers. Participants in the consumer survey in the US watched a video and read information describing the Mobile Connect solution. They were then asked how likely they would be to use Mobile Connect as their primary log-in for most websites, apps, and other online services. The response was very positive: 31% said very likely and 40% somewhat likely.

The research drilled down further on the three key aspects of the Mobile Connect proposition:

- 1) **Universal or single log-in for multiple websites**
- 2) **Strong security**
- 3) **Control over personal data**

All three of these value propositions resonated with US smartphone users (see Table 3).



TABLE 3

	Very appealing	Somewhat appealing
Universal log-in: Mobile Connect enables you to easily login to multiple websites using your mobile phone, and just one password for them all	52%	33%
Strong security: Mobile Connect provides stronger security than current log-in systems thanks to the unique combination of your phone and its password	47%	37%
Control over personal data: Mobile Connect allows you to log-in anonymously or those services that do not require to know your identity.	52%	35%

Universal log-in for multiple websites

More than half of the surveyed consumers found Mobile Connect’s potential to enable individuals to log-in to multiple websites using a mobile phone, and just one password for all the sites, to be “very appealing”. A further third described this proposition as “somewhat appealing” (see Table 3).

Strong security

More than eight out of ten (84%) of US smartphone users welcomed the Mobile Connect promise to deliver stronger security than current log-in systems through the combination of the consumer’s phone and a PIN – two-factor authentication (see Table 3).

The research also found that US consumers are looking for greater protection from identity theft and associated fraud. By utilising mobile operators’ secure network assets, Mobile Connect is able to provide advanced protection against identity theft as well as secure reliable verification of identity. These features appealed to almost 90% of the people participating in the survey, with more than half describing them as “very appealing” (see Table 4).

TABLE 4

	Very appealing	Somewhat appealing
Mobile Connect provides advanced protection from the growing threat of identity theft	53%	36%
Mobile Connect provides a more secure verification of your identity - proving you are the real you	52%	35%

Control over personal data

US consumers are also looking for greater control over their personal data. When they were introduced to the Mobile Connect proposition, 85% of respondents liked the idea of being able to manage permissions for sharing their personal data with online services. More than half described this concept as “very appealing” (see Table 5).

Most of the respondents also welcomed the concept of a ‘personal data vault’ (which could be supported by Mobile Connect in future), that would allow you to collect, manage and control your personal information. There was also considerable enthusiasm for a consistent set of privacy guidelines across service providers (see Table 5).

TABLE 5

	Very appealing	Somewhat appealing
Mobile Connect allows you to manage permissions for sharing your personal data with online services.	51%	34%
Mobile Connect creates a personal data vault that allows you to collect, manage and control your personal information	44%	41%
Mobile Connect’s partner services must adopt the same set of privacy guidelines, reinforcing your privacy and control	49%	37%

4. Example use cases

In the consumer survey, US smartphone users were presented with various scenarios in which Mobile Connect could be used. The vast majority of respondents were interested in these use cases (see Table 6).

TABLE 6: % TOTAL INTERESTED

Reduced risk of identity theft and credit card fraud by increasing the security of all your financial transactions online and in the store because your bank and payment providers can quickly check with you	86%
For almost all login scenarios, just one strong password to remember that delivers high security, instead of having to remember dozens of potentially weaker passwords	84%
Real-time parental control of your family's login to online services	83%
Shorter wait times or queues and better service at call centres, enabled because Mobile Connect allows you to pre-identify yourself	75%
Easier and more secure authorisation of online banking transactions without the fuss of using 'card devices', and filling in long forms to prove your identity	75%
Auto-fill online registration forms or payment details from the information held by your mobile	74%
Alert your bank that you are roaming in a specific country so that you don't run into any problems with using debit or credit cards abroad	70%
Personalise ads based on your own personal information, under your control, rather than on the assumptions of major internet players	66%

In the interviews, the service providers were presented with various use cases for Mobile Connect. In the US and other advanced markets, banks and government agencies were particularly interested in using Mobile Connect to check an individual's location (roaming verification). Banks were also very interested in using Mobile Connect to check various aspects of the customer's mobile account to counter fraud.

The retailers interviewed showed particularly strong interest in deploying Mobile Connect to support user segmentation by location and geo-fencing (determining when a consumer is in a specific geographic area). For online media companies, age verification is a key use case.

This section briefly outlines three of these potential use cases.

User segmentation and location

Once a consumer has logged into a web site or an app using Mobile Connect, the solution can allow them to securely share specific attributes, such as their location, with the service provider for a specific purpose. Through Mobile Connect, the mobile operator would relay this information to the service provider on an anonymised basis. A retailer, for example, could then use this information to provide personalised information and offers tailored to that particular individual's location. For example, the consumer might receive a message about a one-day promotion at a nearby store or an offer for same-day delivery on a product they have been looking at online.

The interviewed service providers described dynamic location information as particularly useful. "Definitely interested in this," one service provider told interviewers.

Age verification

Once a consumer has logged into a web site or an app using Mobile Connect, they could use the service to verify their age. Their mobile operator could, for example, confirm they are an adult to the service provider, which could then tailor the content and information it displays accordingly. This process could be used, for example, to ensure children aren't able to access films and TV programmes that have been certified as being for adults-only.

Retailers, online media and web-based gaming services all showed interest in using Mobile Connect for this purpose. They regard the solution as more reliable than existing age verification methods, helping them meet their compliance obligations, reducing the return rate (parents returning purchases made by their child) and improving their reputation.

Fraud scoring

Mobile Connect can enable a consumer to share some of their mobile account details with a bank, government agency or another service provider that wants to check that they are who they claim to be. For providers of valuable services, the more information they have, the better their ability to detect fraud and reduce their risk exposure. "More [information] is definitely better," noted one interviewee in response to this use case.

Rather than using Mobile Connect to enable the consumer to give their explicit consent to each request for information, the interviewees envisioned that Mobile Connect could be used to provide a straightforward opt-out mechanism or provide one-time explicit consent on registering Mobile Connect with the service provider.

5. Conclusions

Service providers and consumers welcomed Mobile Connect's ability to verify and share information, with the consent of users, easily and securely. As it supports interactions across multiple operators and different digital devices, Mobile Connect can help retailers, government agencies, banks and other service providers better engage with individuals through different devices, improving the end user experience.

The findings of the US consumer research suggest that Mobile Connect could be broadly adopted in North America. In the survey, 71% of the respondents said they would be likely to use Mobile Connect as their primary log-in for most websites, apps, and other online services. The GSMA's research indicates that US consumers would feel comfortable using Mobile Connect in a wide variety of contexts and to access a broad range of services.

The specific challenges faced by retailers, content providers, banks and government agencies mean these sectors could be among the major beneficiaries of Mobile Connect: The solution enables them to address the current trade-off between security and ease-of-use. By making it easy for individuals to control what data they allow service providers to access, Mobile Connect can alleviate consumers' concerns about digital services and encourage greater engagement and interaction with them.

In summary, the GSMA's research shows that Mobile Connect will enable online service providers to build a deeper, more trusted and more fruitful relationship with individuals to their mutual benefit.







Secure digital identity is now in our hands



GSMA Head Office
The Walbrook Building
25 Walbrook
London EC4N 8AF
gsma.com/mobileconnect
www.mobileconnect.io
Published: October 2015