Forgot Password?

By Melissa Cogavin, Managing Editor, SCTE

The recent announcement from the FIDO Alliance promises to do away with post-it notes, memorable words and password-reset emails clogging up your in-box, as soon as next year. Forgetful people the world over will be dancing in the streets. Surely it can't be that straightforward? Melissa Cogavin reports.

As the Digital Revolution and daily life rattle along at breakneck speed, between software updates and handset upgrades it's easy to miss the little details. Those small announcements that pop up on your phone fleetingly and are gone almost immediately (often hard to find again afterwards or is that just me), such is the nature of 24 rolling news, the never-ending onslaught of over-reaction to the smallest event, driven by the media whose life depends on your outrage.

It is unsurprising therefore, that the FIDO Alliance press release perhaps did not receive the attention it deserves. It should have received a lot more. FIDO stands for Fast Identity Online and is an industry association launched in February 2013, based in Oregon, in the US. FIDO's membership is jaw-dropping: containing the world's largest and most prestigious brands and the most recognisable household names, on the Board alone sits Amazon, American Express, Apple, Intel, Google, Meta, Microsoft, PayPal, Samsung, Mastercard and VISA.

FIDO's mission is to "develop and promote authentication standards that "help reduce the world's over-reliance on passwords". FIDO addresses the "lack of interoperability among devices that use strong authentication and reduces the problems users face creating and remembering multiple usernames and passwords."

Andrew Shikiar, Executive Director & CMO of FIDO, broke it down for Broadband Journal. "There are three forms of online authentication. It's essentially what you know, like a password, which is knowledge-based. Then there is what you have, which is proven possession, like your date of birth or zip code. Then finally it's who you are, which is inherent, and that's your biometric (your fingerprint, your voice, your face). Multifactor authentication has, by definition, two of those things. Our initial second factor thing is a what you know plus what you have. But all you're doing is literally touching this thing. It's proving that you're in possession of the device."

Shikiar says this new announcement means there is "a new approach on top of the existing FIDO specs that are being taken by Apple, Google and Microsoft, that will allow for the private key to be securely synced across their device cloud. Such that if you log on with one device, say your MacBook, and you log into your bank account there, then you log into Amazon via your phone, for example, then you go to your other MacBook, all you need to do is present your biometric and your logged into that website immediately."

Jared Newman, a US based technology journalist summed the transition up this way in a recent article in Fast Company magazine. "Imagine, for instance, that you want to create a Twitter account. Rather than making you set up a password

> **It's essentially what you know, like a password, which is knowledge-based. Then there is what you have, which is proven possession, like your date of birth or zip code. Then finally it's who you are, which is inherent, and that's your biometric (your fingerprint, your voice, your face)**

inside the Twitter app, your phone will generate a hidden passkey and store it securely on the device. Twitter itself never learns or stores the passkey; instead, it receives a credential from your phone that verifies your identity and lets you log in."

This is welcome news of course. Human behaviour is nothing if not predictable; how many of us have re-used passwords, knowing we should know better? Who hasn't heard ruinous stories of corporations whose entire IT security system relies on the laughable identifier "Password123"? How many of us have used our children's birthdays, pet's names and mother's maiden names to identity ourselves? Forgetful people the world over will collectively be breathing a sigh of relief.

Currently, society is broken down like this. Organised people might have some sort of password system, a prefix and a changing suffix for every website they access, for example. Others write their passwords down. Big tech is helpfully suggesting customers rely on the 'STRONG PASSWORD' option, offered up by their handsets to do the work for them.

However, there is a worrying number of people who lack sufficient know-how, organisation or awareness and are sleepwalking into a world of well-documented trouble. At best they risk a protracted period of inconvenience and uncertainty while they assess the damage done by using 'Fluffy100' for all their website passwords; at worst, they risk data breaches, fraud and identify theft every time they log in.

Shikiar laughed ruefully. "The best thing you can do in the short term is use a password manager, and that's an imperfect technology. Writing down passwords and sticking them in a drawer somewhere in your home is okay, but not the best practice. It's probably better than leaving it on a sticky note. There's really no great answer. The only right answer is for us to get past this stage as soon as we can. Passwords are simply not fit for purpose for the way we use the internet today."

In the same way we now laugh at what we had to do to load up rudimentary computer games on the ZX Spectrum, using a tape recorder and a tangled spaghetti of wires into the back of a TV in the 80s, the current entry system into websites in 2022 is ridiculous, tedious and certainly overdue an upgrade, never mind the security implications. We will look back on this period with incredulity.

Shikiar elaborated the point. "It is so stunningly easy at the moment to execute a remote attack at scale that we need to raise the bar to a bare minimum. Right now, if you go to the dark web there are phishing tool kits with customer support available for just a couple of hundred dollars. I can get a toolkit that allows someone to create a fake banking website for me in no time. These are phishing websites, phishing tools, giving access to stolen lists of emails and email/password combinations where I can start spraying people. It's that easy. You're always trying to stay ahead of the hackers, and I think that will always be an ongoing task. But this development stands to raise the bar dramatically."

These new capabilities are expected to become available across Apple, Google, and Microsoft platforms over the course of the coming year.

It is fair to say that while Big Tech are again racing ahead in the name of progress and they are to be congratulated at working collaboratively on a massive scale, there are implications to consider. Broadband Journal talked to award-winning music journalist and broadcaster Pete Paphides, whose father passed away recently.

On Twitter Pete recounted a sad story about his own 84-year-old father, whose failed experience trying to pay for parking via an app a few months ago on his phone eventually led to a disproportionate fine. He spent the last weeks of his life unsuccessfully trying to resolve this, a problem his family had to sort out once he had passed away. The post went viral and led to a broader debate about communities being left behind as technology advances at a faster pace year on year. "It's out of control," Pete said. "Tech companies can't or won't govern, and governments don't understand the technology." We have covered the glacial pace of legislation in this area in other Long Reads – the issue is the same here too. All of

which leaves marginalised groups even further at the margins, frustrated and unrepresented. “Exactly. All those years of learning, education, experience that my dad had, and he was made to feel obsolete.”

Pete’s dad was unable to navigate one of the various parking apps now replacing pay and display machines across the country. Unless you have a smartphone and a credit card and unless your mobile phone contract contains a built-in data allowance, pay-as-you-go customers must rely on BT Wi-Fi, which is expensive, payable by the hour/day via credit card, and not always compatible with downloading and managing apps. Pete’s dad did his best, standing in a car park in the open air in a hurry to get to his friend’s memorial service, but was unable to pay for the parking and received a £170 fine shortly afterwards.

Pete explained, “Dad called me the next day in a panic; he did what he could to sort it; he was a proud man and it was humiliating for him. He found himself asking around for help. He spent countless hours on hold, via chat bots and people in call centres who must realistically be dealing with this situation in their thousands every week, but there is no option to solve this issue anywhere. I’m 52 and it wasn’t exactly intuitive for me, what chance does a man in his 80s stand?”

On an emotional level it is tempting to assume phone companies find it easier and perhaps irresistible to exploit pensioners for failing to keep up than create a provision for people who don’t have the technology or the know-how, but is that really the case?

Sally West is a Policy Manager at Age UK and explained how the complex the issue is. A lot of work has been done in this area, there are education and training schemes available aimed at equipping seniors with the IT tools they need, but there is a woeful gap between what is happening now and what needs to happen to ensure modern life is as inclusive as possible. There is also the important point that some older people are unwilling to engage with technology, regardless of the training on offer. In a recent study, the charity found that despite the pandemic forcing us to move increasingly online, “it does not appear to have made a substantial difference to the proportion of older people using the internet.”

In early 2020, “Among those aged 75+, more than two out of five (42%) did not use the internet. Only around a quarter of this age groups (24%) said they were using the internet more since the pandemic while nearly one in ten (9%) were using it less. Even if people use the internet they may only do so for a limited range of activities and may not have the latest technology. For example, in early 2020 just 53% of people aged 65+ in Great Britain used a smartphone for private use compared to between 95% and 98% for those in age groups 16-24 up to 45-54.” It is clear therefore that FIDO’s announcement, while well-intentioned, will have not landed with almost half of the 65+ demographic in any meaningful way.

Using the internet is not like riding a bike, Sally added. “It’s a case of continual learning. Technology is changing constantly; you need to keep using the internet to keep up with those changes. Sensory and cognitive decline increases as you get older. People get slower and react slower. It’s hard to keep up, even if you want to.” (NB: that’s not just the elderly. Professional gamers retire from competitions at 26 on average; their own cognitive abilities have declined to an extent that they can’t keep up with teenagers ten years younger. Any parent trying to keep up with a child playing a game on an iPad will probably agree). Those who leave the workforce adept at using the internet are better placed to face retirement in an online world than those who are learning from scratch once they retire. There are also cost barriers to consider; smartphones are expensive, as is internet access, and if you have never needed either before it all seems a bit of a lavish indulgence that won’t be used to its full potential anyway.

Combine all the above with a noticeable shift towards a cashless society since the start of the pandemic, and we are back in that car park with Pete’s dad.

Passwordless authentication does not take into account developing countries or various states of literacy in those countries either. Teddy Woodhouse is a Senior Research Manager for the A4AI, the Alliance for Affordable Internet, a global non-profit organisation containing many of the same blue-chip members as the FIDO Alliance, and is concerned with the equitable provision of internet access worldwide, specifically focused on developing regions such as central and South America, and Southern and Southeast Asia.

“Our broad ambition is that everyone should have 4G access to the internet. They should have a smartphone and they should have high-capacity connection at some point in their daily life, usually home or school.” The concern with the FIDO announcement, he feels, is that smartphones are far

from ubiquitous in developing countries and passwordless authentication will only widen the gulf between the rich and poor globally. He is positive about it, but it seems a remote destination given his current remit.

"In terms of thinking about the privacy aspects [of internet access], there are some ways where we at A4AI touch upon those issues and generally, it fits within our broad approach of favouring consumer rights and encouraging consumers in encouraging governments to create protections for those consumer rights to be protected. That can span from things such as mobile number portability, which is kind of a closer issue to us."

Their more immediate issues are around affordability. The A4AI graph below illustrates just how irrelevant passwordless authentication is in LDC's (less developed countries), where ownership of a smartphone is so prohibitive at over half their monthly income, it renders the possibility fairly unlikely at all. That's in addition to domestic internet access, Teddy explains. "You can start to see the huge disparities between the richest who are paying fractions of a percent of their monthly income to afford data, versus those at the bottom who are having to pay up to 30% of their monthly income." 80% of household income on a phone and data in developing countries? FIDO's hopes and dreams are a world away from the real life of A4AI's gloomy statistics.

Down the line, Teddy diplomatically argues, it is good to see these measures kicking in in the developed world as ultimately the benefits FIDO are pushing for will trickle down to the Pacific Islands, for example, but it is a long way off. In countries where there is a distinct gender imbalance, such as the now Taliban-controlled Afghanistan, women and girls are prevented from receiving an education at all, so their access to the internet is prohibited by them being even able to read.

Another concern is personal security. This latest announcement effectively places our own identities into the hands of a few big tech companies; should we wish to migrate from an iPhone to an Android phone, for example, moving all our passwords over is not straightforward. For those of us using the internet all day every day in our daily lives, that could mean hundreds of passwords, and FIDO admit that in their mission to provide internet security and prevent hacks, their provision currently falls short. This means those passwords will have to be manually moved across one by one. Such a process could take customers weeks, months, if it happens at all. Laborious and off-putting it certainly is, and it will almost certainly prevent that kind of fluid movement between providers that consumers

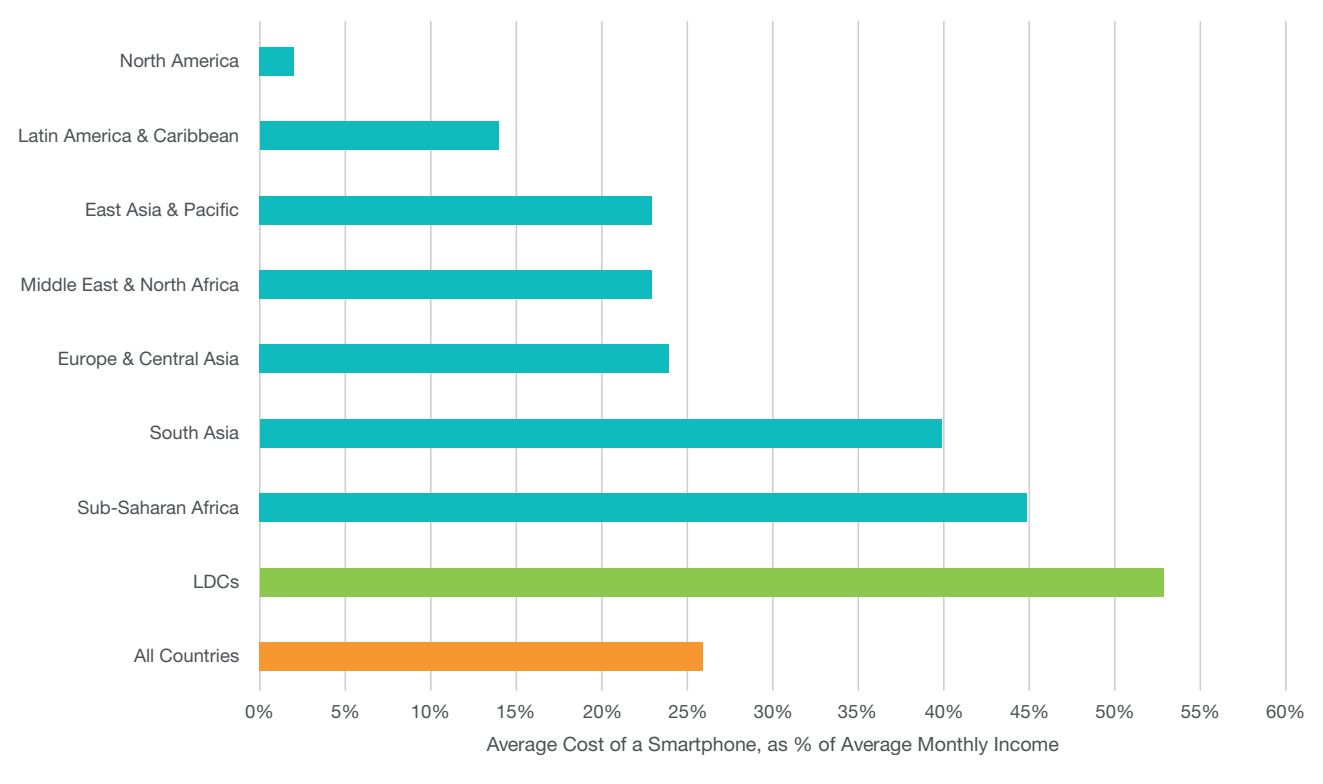

Figure 1: Smartphone Affordability by Region. Source: Alliance for Affordable Internet

FIDO have stated that locking people in is more related to security and they are working on a 'future iteration' making it easier, but they haven't exactly pinpointed a date when that future iteration will be available.

ought to have at their disposal. Duplicate accounts are a likely outcome instead.

Jared Newman has a few thoughts on this. "I'm unusually paranoid about being locked into technology," he told Broadband. "Handing over passwords to a huge company so they become a single 'passkey' that we never see means they are taking control out of the hands of the user and into the hands of the platform itself. I'm uncomfortable with this. I want to be able to move from Android to iPhone, from Microsoft to Apple freely." As the user is after all paying for this privilege, it is a fair point, and not an unreasonable expectation. Does he think there is some malevolent intent going on behind the scenes?

"The quantity and reputation of the stakeholders within the FIDO Alliance means probably not, so we have reason to be optimistic. FIDO have however also stated that locking people in is more related to security and they are working on a 'future iteration' making it easier, but they haven't exactly pinpointed a date when that future iteration will be available. It isn't in the interests of Google, Apple, Microsoft, Samsung and so on to do so." Jared feels there is a conflict of interest at work, with the end-user feeling the pain.

Rather like the recent Long Read on the Internet of Things, which explored the degree to which the user is happy to part with their own personal data in exchange for Alexa turning the lights on and playing their favourite radio station, the handing over of our password manager to a faceless corporation could have ramifications down the line, if anyone can be bothered to investigate it more closely. The likelihood is, most of us will tick yes to the terms and conditions and get on with our day.

The scenario painted overall is emblematic of the evolution of the Internet itself. Unfeasibly vast, almost indefinable, owned by nobody, completely unregulated but despite everything, widely acknowledged to be a force for good. It is heartening to see Big Tech and FIDO grappling with internet security as part of a broader initiative to reduce cyber-crime and implement some global standards, but it is equally understandable why it's taken nearly ten years for FIDO to get this far. In researching their achievements, one has a clear sense of a salmon swimming upstream throughout.

The trickle-down positive effects of FIDO's efforts will be welcomed but it may take yet another ten years, plenty of confused dads like Pete's along the way and millions of frustrated iPhone users tied to handsets they can't easily escape from in the meantime for the wrinkles to be ironed out. On a more positive note, ten years might see the upside-down economics currently facing less developed countries right themselves sufficiently to take advantage of the efforts FIDO is making on a local level.

FIDO's ambitions are laudable, and they must be recognised for the work they have done in this area so far to regulate the hacking that causes pain and suffering to millions of hapless users every day. The Internet was an unplanned initiative and has ballooned in a very short space of time. The grandfathers of its evolution are still very much with us, and not even elderly men themselves yet. Taking a step back to evaluate its history and development, FIDO's work is a vital foundation that will build on itself and prove its value substantially over time, but there are hurdles to get over and important questions to be answered as this process continues.