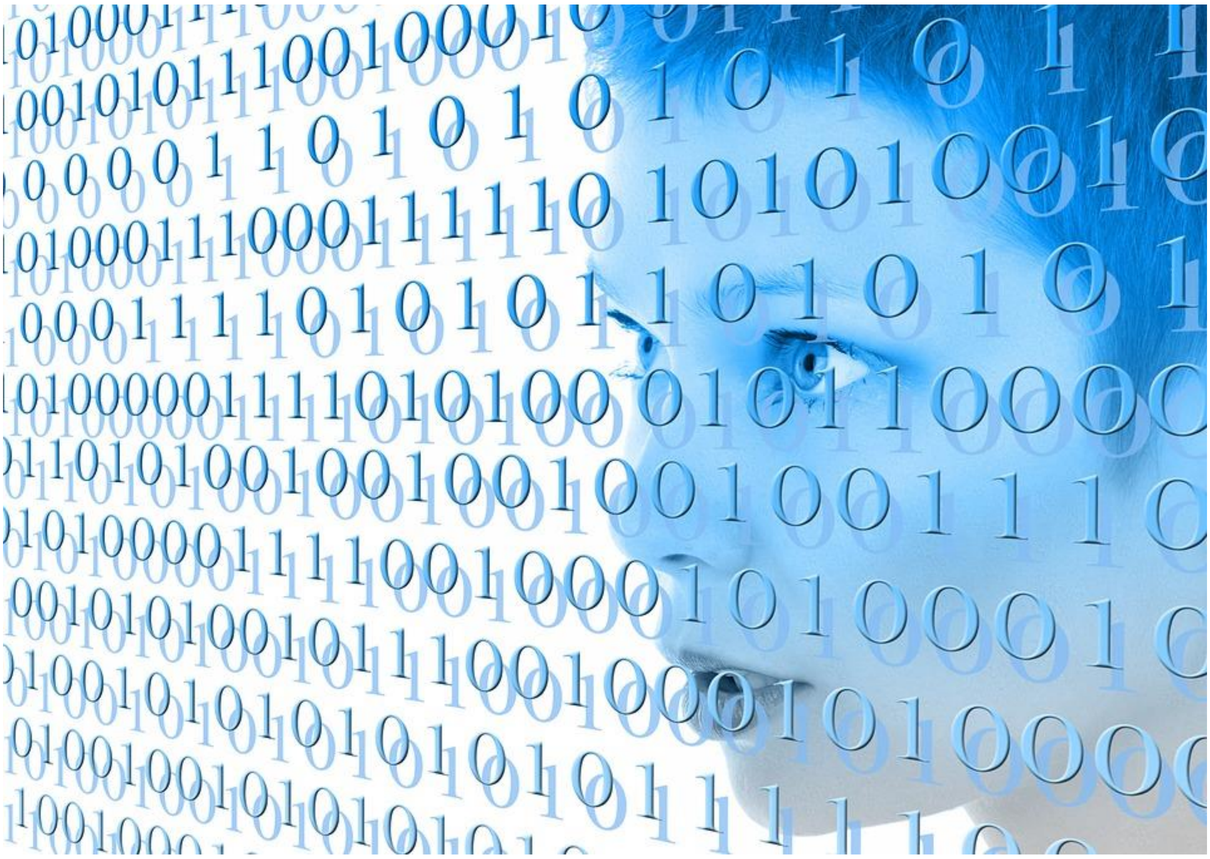
Digital Wallets: Impacts, Implications and Issues



https://pixabay.com/illustrations/digital-zeros-ones-woman-stylish-388075/

Prepared by Dr Jill Bamforth (Lead Chief Investigator) on behalf of:

Professor Anita Kocsis (Director, Design Factory Melbourne); Associate Professor Prem Jayaraman (Head Digital Innovation Lab Swinburne University); Dr Amir Andargoli (Innovation technologies expert); Dr Hadi Ghaderi (Optimisation and digitalisation expert); Ms Bridgette Engeler (Futurist expert); Dr Barbara Bok (Research Assistant)

Disclaimer:

This report (including any enclosures and attachments) has been prepared for the exclusive use and benefit of the addressee(s) and solely for the purpose for which it is provided.

The content of this report is based on information gathered in good faith and ethical manner from secondary sources and it believed to be correct at the time of publication.

We do not accept any liability whatsoever if this report is used for an alternative purpose from which it is intended, nor to any third party in respect of this report.

It's that privacy, you know, protecting the privacy of everybody that I think needs to be front and centre of all this technology (Participant 12)

https://commons.wikimedia.org/wiki/File:Onlineidentity.png

Executive summary

This report covers findings from Stage 3 of a co-funded Swinburne University/460degrees research project into the social and psychological enablers and barriers to digital wallet usage which ran from August 2019 to April 2020. Findings suggest a tension between convenience and concern that affected perceptions of trust in the digital technologies.

Key findings

1) **Psychological and social factors affect perceptions of trust -** There was a wide variance in what constituted the boundary between private and public personal data. This affected what type of data should be shared and protected, and the level of control each participant felt they needed over their personal data and its usage. Factors increasing risk tolerance were a broad understanding of how the Application (App) worked; trust in the App provider; choice in App usage, what personal information was shared and who had access; ease in recovering lost or temporarily forgotten data; and other broad influencing social and organizational processes (e.g. cultural expectations, established institutional loss recovery processes, and business, ethical and profit motivations).

2) **Perceived benefit from sharing data** - In most cases, concerns about the collection of personal behavioral data on phones or smart devices for use by third parties were balanced against the perceived personal benefit the App/device provided. Acceptance or tolerance of personal data sharing to third parties appeared to increase when Apps enabled easy satisfaction of a defined and valued personal benefit whilst offering individuals control and flexibility over their privacy settings and choice over how their personal data was collected and used.

3) **The Melbourne Wallet** – There was a mixed reception to the idea of a Melbourne Wallet with a lack of clarify about the value it could offer to locals or internationals. This suggests its utility needs to be clearly identified and its benefit promoted through a group of influential early adopters.

4) **Smart Cities and the IoT** – There was a range of feelings about smart cities underpinned by themes identified elsewhere in this report. Areas of concern were around protection of self and loved ones; data collection and usage; and intrusion into the home (considered by many to be a private area). Potential benefits identified were linked to greater convenience and increased accessibility to products and services felt to deliver personal value.

5) **Additional research** – This research suggested trust was a key consideration with concerns about risk being mitigated by the meeting of a perceived personal need, some control over privacy of personal information, reputational trust in the provider and an easy to use App design. Whilst few participants directly considered what constituted social trust, across all participants there was an assumption of properly functioning social processes. There was a lack of critical reflection on current or anticipated future social processes, particularly in regard to the implications of technology. Further quantitative research is needed to uncover the relevance and importance of each in the mitigation of risk. Additional quantitative research is needed to identify the prevalence of these findings amongst the broader Public.

Contents

1.0 Introduction

The advancements in technology provide an opportunity to replace physical wallets with a digital version. These are called an “e-wallet” or “digital wallet”, or when used on smartphones a “mobile wallet”. A review of the literature revealed that most of the studies on this new technology focus on the use of digital wallets for making payments (Balan et al. 2006; Rathore 2016; Taghiloo et al. 2010). This limits wallets to carrying cash and credit cards, ignoring its wider application to the carrying of identity cards (i.e. a driver’s licence), public transport cards, loyalty cards, tokens, and so on.

In addition, the current literature mainly focuses on the technical aspects of digital wallets such as security and privacy (Balan et al. 2006; Ebringer et al. 2000; Ghag and Hegde 2012; Rathore 2016; Taghiloo et al. 2010), architecture (Houngbo et al. 2018; Ravi et al. 2018; Shaghayegh 2011), interoperability (Benson and Loftesness 2012; De et al. 2013; Neeharika et al. 2014), and costs (Alkhunaizan et al. 2012; Comninos et al. 2009).

Limited research has been done on the human behavioural aspects involved in the adoption of digital wallets which have been largely overlooked in the literature. The public’s usage of Web based Apps is growing exponentially as they become more embedded into Australian life. Therefore, our research explores how digital technologies affect autonomy, competence and relatedness, particularly self-control, need satisfaction and individual well-being. In the process we touch on how digital technologies affect family relationships, leisure activities, work, commerce and the consumption of mass.

The ongoing impact of the Covid-19 virus on how society digitally works and plays highlights the need to better understand the psychological and social adjustments individuals make when they engage with web based Apps. This research seeks to enhance understanding of the positive and negative aspects of digitisation and interconnectivity at a social and psychological level for individuals and groups. This project leverages current knowledge and literature on self-sovereign identity (SSI), an emerging open sourced platform, to determine the minimum functionality needed for Melbournians to maximise the use of a digital wallet. SSI is the next step beyond user-centric identity (Tobin and Reed 2016), placing the individual at the centre of their identity administration by making their identity independent of identity providers. SSI therefore creates user autonomy returning control of personal data and digital appearance to the individual (Der et al. 2017). SSI offers a persistent, portable, interoperable, and secure (Der et al. 2017) mechanism allowing the interoperability of a user’s identity across multiple locations with the user’s consent ensuring that digital identity is transportable and not locked down to one site or locale. SSI enables users to make independently verifiable identity claims about their person, capability or group membership, moving beyond digital payments.

The research was jointly funded by 460degree Consulting and Swinburne University through a $40,000 Research Seed Fund grant awarded in 2019.

The research team consisted of: Dr Jill Bamforth (Lead Chief Investigator); Associate Professor Prem Jayaraman Head Digital Innovation Lab Swinburne University); Professor Anita Kocsis (Director, Design Factory Melbourne); Ms Bridgette Engeler (Futurist expert); Dr Amir Andargoli (Innovation technologies expert); Dr Hadi Ghaderi (optimisation and digitalisation expert); Dr Barbara Bok (Research Assistant). The team also acknowledges the important contribution that Dr Andrew Roberts made during the team’s formation; and reports by Professor Jeni Paay’s outstanding capstone Design students.

The project adopted a co-design explorative approach with members of the Public and the research team to uncover and evaluate the issues, opportunities and challenges of using a digital wallet (e.g. a Melbourne Wallet) within a smart city ecosystem. In this context a digital wallet is defined as a digital version of a physical wallet where physical cards can be stored digitally but which may also incorporate other Apps. The design of a digital wallet design should therefore enable the delivery of content in a way that protects users' digital identity whilst providing a sense of safety, confidence and security.

The research adopted a multi-stage project approach and was undertaken between August 2019 and June 2020 as follows:

- **Stage 1 (August 2019) - Three scoping workshops** consisting of digital and design experts from 460degrees Consulting and Swinburne University to identify what was and was not known about factors relating to digital wallet take up and usage. Findings informed the parameters of the study.

- **Stage 2 (August – October 2019) – Final year undergraduate design students Capstone Project**. Students explored, through their personal connections, how digital wallet take up and usage could be enhanced through design.

- **Stage 3 (December 2019 – February 2020) – 17 interviews** with members of the Public to explore the social and psychological aspects of digital wallet usage.

- **Stage 4 (January 2020) – 2 co-creation workshops with 16 members** of the public to explore
  - How participants' use Apps and digital wallets in their day to day life
  - The problems digital wallets pose for users and how these could be overcome
  - What an ideal digital wallet might look like
  - What features make Apps and digital wallets attractive
  - What strategies could be used to encourage greater usage of digital wallets

F**indings from stages 1 and 2 were used to inform the data collection approach for stages 3 and 4** (open-ended interviews and workshops). Participants for these latter stages were drawn from a range of different socio-economic backgrounds and sourced through Swinburne University staff networks. Data from the interviews and focus groups was initially thematically analysed by hand to identify central themes. Deeper analysis will now be undertaken using Nvivo software to explore these themes further in preparation for research publications post project.

This report focuses on the Stage 3 interview findings.

2.0 Interview Approach

Interview Approach taken to identify social and psychological aspects of digital App usage

Participants were asked to identify what Apps they had on their phone and why. The purpose of this discussion was to identify comfort with technology usage and the factors enabling and discouraging App usage. Participants were then asked about their physical and digital wallet usage and their comfort in operating only with a digital wallet. This opened up discussions around convenience and trust, exposing underlying social and psychological considerations. For each participant a conceptual map of key themes was constructed, and these themes were then compared across the participants and used to inform subsequent ongoing interviews.

3.0 Interview Findings

The interview findings on the social-psychological aspects of using digital wallets are reported against the following categories:

- Diversity of app usage and words used to describe them
- Emerging themes
- Factors mitigating lack of trust
- Appetite for the Melbourne Wallet
- Smart cities and IoT
- Future Research

3.1 Diversity of App usage and words used to describe them

Participants used a wide range of Apps covering social media, banking, lifestyle, arts and culture, sports, shopping, music, utility, gaming etc. The use of Apps was viewed as both enabling and threatening to participants. Table 1 highlights the range of social and psychological descriptors used by participants to describe their engagement with Apps.

Table 1: Descriptors used by participants to describe Apps/Digital Wallets.

	Positive words/phrases	**Negative words/phrases**
Social Factors	Connector to family and friends; serves the purpose of more [national] security; more peace of mind; our choice to share; responsible purchasing; know what the process is for recovering data.	Distracting, time waster; no other alternatives; forced to upgrade; forced to sign data over; digital footprint there forever; once posted can't get it back; authority owns me; tapping into people's insecurities; culturally, we just have a deep mistrust
Psychological Factors	Simplifies life; easier; convenient; $800 pocket computer; efficient; freedom of choice; have a choice; share my lifestyle; responsible purchaser; shows the owner [options]; [reduces] pieces of paperwork; gives me ownership back; keep track; amazing; excuse to hang out socially; build my own brand	Invasive; overwhelming; paranoid; annoying; dependency; fear of forgetting phone; fear of flat phone battery; risky; don't have a choice; spooked; paradox of choice; panic stations; forced to use; not a responsible purchaser; lost all that information; digitalize all my assets; [cash allows you to] touch it, sense it, you see it, you can count it; lost my skill at handwriting; survived 10 years ago without it.

3.2 Emerging themes:

Trust in the technology and the protection of personal data was a central issue. However what aspects enabled or destroyed that trust were highly individualised across the participants.

These aspects are grouped as follows:

Aspect 1 - **What constituted core personal data** that should be protected

Aspect 2 - **The perceived level of personal control over App engagement**.

Aspect 3 – **Trust in the App provider protecting personal data**

Aspect 4 – **Whether individuals felt they** personally **had anything to hide**

These are discussed in more detail below:

3.2.1 Aspect 1 - What constituted core personal data that should be protected

All participants spoke of protecting their personal data, location, family, friends and personal resources but the level of concern around what should be protected and why varied.

Some participants identified 'high risk' data as: key identifying data which was difficult to replace and which when leaked would likely lead to identity fraud and significant disruption to personal life e.g. passport, driving licence, health card information. This group were careful with their personal data.

> *I think [I would upload] bank cards, Myki cards, the stuff I use every day, but I think Medicare card, passport, driving licence – no - I would worry about security, people just accessing everything and I know they can access everything about me anyway but I think that would be making it far too easy for hackers to hack my entire life.... not things like passport, Medicare card because that's kind of like your whole identity. (Participant 16)*

> *The trade-off that I will lose my personal. I can't. I will lose my personal information and people can use that for inappropriate purposes. That's why I closed my Facebook and that's why I don't keep my Facebook public to people. (Participant 3)*

> *I think in Australia in general, there's like deep mistrust in the government and in the private sector [to protect data, and that is why] on social media, I've given misinformation, so a lot of my details are incorrect. Well, they're all incorrect. So I feel I've somewhat de identified myself. (Participant 9)*

At the other end of the scale were individuals who, although aware of data theft and identity fraud, stated they were not overly concerned. This group ranged from those ready to move all their physical cards online for greater convenience to only those who would put some cards online.

Reasons given were:

1. they felt that they personally had nothing to hide and therefore did not need to be concerned about what data was collected or how it was used
2. they felt unable to control what data was collected about them and how it was used and so chose not to think too much about it
3. they felt the App provider would protect their data because to not do so would damage the organisation's reputation

I believe that somehow with this new technological revolution, and the internet and all that sort of stuff, that if somebody wants to find something out about me, they probably will. And that doesn't bother me. Because I'm just a realist, and I'm like ,oh well, and also because I don't think there's really anything that exciting to find out…. I'm sensible though. I don't do stupid things like take photos, I don't use Facebook as an advocacy platform (Participant 13).

3.2.2 Aspect 2 - The perceived level of personal control over App engagement

This aspect covers how much perceived choice an individual felt they had over their engagement with an App. It includes what data an App could collect and use for profiling; the level of targeted advertising allowed by the individual and what personal information an App could share with others.

If they want to serve ads [adverts] at me that I find relevant, or if they want to recommend a concert to me or, or something like that, based on my previous behaviour on their site, then absolutely go for it. I think for basic purchase decisions like that I'm still capable of making up my mind as to whether I continue on with it. It's obviously only when they get into the realms of taking your data without your consent [that I get worried]… (Participant 5)

All participants were aware that their online data generated unintended data by-products during the application of technology to specific tasks which could be mined by App and other third party providers. Awareness of this data collection and its usage by organisations unearthed a number of psychological considerations, broadly falling into fear about dependency on the technology and loss of control over that technology and personal data.

Distrust in the technology either arose because the technology demanded a behaviour that either did not align with existing preferred and trusted behaviour/personal logic frameworks (e.g. a phone swipe pay versus a card based tap and go approach; or a pin being required for transactions under $100 but not those over $100); or the user did not understand how the technology worked on their phone. This meant they were unable to gauge the level of risk from using this particular App on other data held on their phone.

When I, go to Meyer, my MeyerOne card is on here, and I scan that. Right so they just scan that, but all they're scanning is a barcode so I understand that, I'm not tapping anything, just scanning a barcode. So that makes perfect sense to me. Because I'm of that era, and I understand that technology, I know how it works. But when I log into [an App I'm not familiar with], I don't understand how that works. So am I giving you access to my bank account? (Participant 12)

Insecurities arose from fear of dependency on the phone and a fear of loss/reduced accessibility to personal data and App functionality. This could arise from limited digital capability, limited cognitive understanding of the technology or limited phone capability. Transferring between devices, software upgrades and having a phone hacked were identified as potential 'loss of data' events.

I'd keep my credit cards and my EFTPos cards, here [in my physical wallet]. I'm always scared if I lose my phone, and I don't have all this to back me up. (Participant 8)

Concern was expressed about the negative impact of the technology on personal/family assets and reputation such as fear of not being able to adequate curate ones' personal image or personal postings online. Feelings of being overwhelmed arose from App variety; lack of confidence in App usage; security issues and scare stories from family, friends and the media which often led to a sense of disempowerment. One participant concerned about human rights and climate change spoke about feeling unable to influence outcomes because of a strong established system.

My generation were very much concerned with the current state of everything really. Starting from politics, human rights, environment. And to be honest, we feel that we can't change anything because of this system that is very, very strong system, you know. And yeah, we sort of live in this fear really (Participant 6)

3.2.3 Aspect 3 - The trust the participant had in the App provider protecting their data

Distrust in the App and/or institution/organisation behind it influenced how participants felt about the collection, aggregation, usage and sharing of their personal data. Data collection issues arose from data collection without explicit consent (e.g. tech's passive listening abilities); perceived coercion to divulge data (e.g. signing up and data scanning) and a perception that increasing data digitisation would encourage society to collect it, whether it was needed or not. Aggregation of data was perceived a personal threat by a number of participants, particularly where that led to the potential revealing of lifestyle preferences and sickness they did not wish to share. For these participants, the need to explicitly understand the profiling process and outcomes was needed to establish trust in the custodian capabilities of the App/Institution/Organisation. **Distrust in an organisation (e.g. Google) or App (e.g. Facebook) led participants to either use the App in a curated way that protected their personal interests or to source alternative options**.

> *I suppose it depends where it came from [face recognition]. If Apple released it, for example, because I trust Apple, I'd probably be, be fine with that. But if Facebook was to introduce it, I feel like I don't have the same level of trust for Facebook then so I, I might not be quite as, as trusting. But in saying that, yeah I'd probably adopt it. I think companies that big rarely make mistakes that large, or that particularly at this point in, in their history. (Participant 5)*

> *My barriers for privacy mindedness are kind of different on a personal and institutional level. Personally, I don't want anyone looking through my stuff. Institutionally. I do what I can so that they're not gaining more information about me than I give them. But I also understand the fact that […] in order to block [e.g. threatening or illegal] content, Facebook necessarily has to scan every piece of content that comes through, which means that it's reading everything I do. […] Like, I'll, I'll allow Facebook to do it, but I wouldn't allow my friend to do it (Participant 4)*

Participants perceived targeted adverts as an advantage (saved time looking), annoying (don't want to be bothered) to worrying (how do they know that about me). Participants significantly concerned about protecting their privacy and confidentiality, carefully managing their public profile, their personal groups and what they posted. For example all participants used social media sites but the level and type of usage varied. Instagram was the preferred social media App as it was easy to use, and gave users a sense of control over their data and image. Participants felt able to curate and protect their personal brand; passively follow influencers or connect to interest groups; activities; and goods and services. Instagram was seen as offering significantly more functionality and security than the older Facebook technology, not helped by Facebook's lack of transparency about data privacy and negative publicity on data breaches.

As already noted distrust in particular functions offered by an App also led to their selective use. For example all participants used bank Apps to monitor accounts and transfer money between accounts. However some participants chose not to use particular banking functions because of a lack of trust in the functions ability to ensure adequate data protection. For example a couple of respondents stated that because they were unclear about the mechanics of phone tap and pay, they did not use this App feature as they felt unable to adequately assess the level of risk this function posed to other data held on their phone. One participant used their mobile only as a back-up for their physical cards. Those with significant distrust in an organisation (e.g. Google), App (e.g. Facebook) or institution (e.g. Government) abstained from using those Apps/smart devices.

3.2.4 Aspect 4 – Whether individuals felt they personally had anything to hide

Some participants were happy to reveal information about themselves as they felt they had nothing to hide.

> *I'm comfortable about revealing [my driver's licence] … that doesn't worry me, I sort of feel I have been an honest person, so I don't have anything to hide. (Participant 7)*

However security of data was particularly important for participants who described themselves as ‘private people’ or who had a personal lifestyle or medical condition they did not want to share with others.

It's not because like I'm afraid of like my data and so on. It's mostly because like, I do tend to put on filters with publicly available. Do I want my political presence right out there where all the trolls could like attack me? Or do I want my extended family to know how gay I am? Of course not because they're homophobic. So I put all these filters on so I [don’t] like share everything (Participant 2)

I think of perhaps the clients I used to work with, and I think about […] how perhaps there are individuals who have consented to [having] their children’s diagnosis papers uploaded [and I don’t like how] with those children, I think one day they grow up, they'll look completely different. I don't want them to be having to have that paper trail necessarily with them because of possibly negative bias […] but, personally I, like I'm, I’m okay. (Participant 9)

Without exception, the small number of parents interviewed all adopted a proactive approach to managing their younger children’s digital footprint, including those who had expressed limited concern over collection and usage by App providers of their own personal data. Almost all either controlled, or sought to control, their children’s engagement with Apps or gaming devices and educated their children in digital dangers. A key concern was the long term impact of the digital footprint on their children’s mental and physical safety and children’s ability to protect their personal and professional reputation in adulthood. One participant spoke extensively of the need to adopt, in this context, a ‘right to forget’ legal framework similar to that being adopted in parts of Europe.

So there should be also an age, a data aging. The European Union are onto this with the ‘right to be forgotten’, - I mean, if people have done something wrong or they've had a little issue and it's blown up - in the non-internet age it would have been forgotten, but now it's remembered by everybody and its newly discovered by new people who can be horrified by it however many years later. So whereas your sort of debt to society type of embarrassment at the time should have come and gone, it never does. (Participant 14)

3.3 Factors mitigating lack of trust

For most participants, concerns about the collection of data by phones or smart devices on behaviour by third parties was balanced against the perceived personal benefit the App/device provided. Benefits came from a convenience/fills a need; the reputation of and confidence in the provider/technology; self-efficacy; tolerance of risk; and attractiveness of design. The participants level of need to use those Apps, the perceived need to manage those aspects and how easy the App provider made it for participants to control the level of personal data shared.

> *I do all my shopping on my phone. It's actually a lot easier to do it on my phone than on the computer. Most of the time I will just take my phone. [If I had the option to transfer all my cards onto my phone] I would yup. My phone is on me all the time. When I go into my wallet I need my thumbprint. So that's my security, but to access all my other Apps, anyone can do it. (Participant 1)*

3.3.1 Convenience

Convenience was linked to enhanced quality of life and tolerance of the perceived risk from App usage. For example smart devices could get rid of chores around the house, or aid safety by warning of trip hazards, threats to security etc. Apps that aggregated and streamlined services (e.g. Paypal) or other Apps (e.g. Shopback) were often seen as time savers. Social media offered connection to loved ones and Society – allowing participants to stay connected, up to date on trends and ensure they didn't miss out.

3.3.2 Minimising negative impact

Many participants were happy to trade data privacy for convenience and App usage at no financial cost, as long as they were not overly negatively impacted by doing this. To ensure this participants adopted a number of strategies:

- choosing known providers based on what trusted others were using, and/or their perceptions of the organisation/Apps competency in delivering effective, efficient and safe technology solutions
- trusting their own ability to make informed decisions
- Providing misinformation or aliases
- Limiting technology take up to those technologies understood

3.3.3 Key considerations: Value add, ease of use and customisability

The combination of a clearly identified value add, ease of use and customisability to personal preferences stimulated take up.

> *I really like the idea of a smart house because it just makes your day to day life a lot easier. So anything that can get rid of chores in the house, so like your washing is done and hung up for you. I wouldn't really be concerned about that kind of detail, like what I eat and stuff that doesn't really bother me [but] I don't like the Alexa thing. I don't like smart watches. I don't like Siri, I don't like things that are listening to me. I sound really paranoid (laughs). (Participant 16)*

Easy to use equated to minimum effort. Apps were considered attractive when:

- they were quick and easy to access and navigate through drop down menus (i.e. intuitive);
- allowed movement between areas of the App (e.g. Netaporter);
- had streamlined but not multiple steps (poor examples: Uber, Paystay),
- had clear pictures, text and information.
- They always worked and were fully developed.

3.3.4 An expression of personality

Customising a wallet or how and what Apps were aggregated turned it into a tool to express personality. Flexibility to change/update options prevented things getting boring. Customisability included opt out functions, customisable security setting; automatic back up to the cloud, and options to shape and visually represent important data e.g. daily expenditure.

3.3.5 Examples of Apps that build trust

Examples of Apps that build trust were:

1) **Instagram**: an American photo and video sharing social networking service owned by Facebook Inc. Attractive features included:
    a. A feeling that users were able to bring about small incremental societal change.
    b. Ability to use as a personal branding platform
    c. Ability to easily follow trends
    d. A user friendly interface which built trust
    e. Accessible key information e.g. privacy policy clearly written
    f. Easy to control functions and easy to control everything e.g. easy to change things.
2) **Shopback:** an e-marketplace App (aggregator of online product/services companies). Attractive features included:
    a. Money back on every purchase
    b. Discount paid back into account of choice e.g. Paypal
3) **Hamilton island App**: Hamilton Islands tourist App. Attractive features included:
    a. Wide variety of events promoted for all age groups
    b. Easy to use
4) **Netaporter**: a designer fashion App. Attractive features included:
    a. Visually appealing
    b. Easy to use; make payments; track purchases
5) **Google arts and culture App**: an online platform through which the public can view high-resolution images **and** videos of artworks. Attractive features included:
    a. Linkage to a map so you can navigate to destinations.
    b. Opening times and cost of entrance
6) **Uber taxi** – part of an American multinational ride-hailing company offering services that include peer-to-peer ridesharing, ride service hailing, food delivery (Uber Eats), and a micromobility system with electric bikes and scooters. There were mixed responses to this App but attractive features identified
    a. **Ability to see where the driver was on a map**
    b. Ability to know cost before ride
    c. Automatic pay from account (i.e. no cash).

4.0 Appetite for the Melbourne Wallet

There was mixed interest in the idea of a Melbourne Wallet and participants were unclear about whether it offered more value to international visitors or domestic citizens/travellers. Whilst the digital wallet was considered and interesting idea, more research is needed to identify and explore the utility of the Melbourne Wallet to a specific target market.

4.1 Key Concerns: Utility and Privacy

Two key concerns were raised about the Melbourne Wallet. The first was utility i.e. how are you going to convince people to download an integrated App of stuff they already have elsewhere? The second was privacy concerns. These concerns revolved around potential risk in linking everything together. Some participants were concerned that if you linked everything would that increase the risk to their personal data being hacked or their behaviour being tracked.

4.2 Key Enablers: A strong value proposition; Security options & easy to use

A number of enabling areas were identified – clear identification of a need that can be filled; how to encourage take-up; and design aspects to enhance usability.

As discussed elsewhere in this report many participants argued that a strong value proposition was needed focusing on the benefits offered in order to move people from their status quo positions. The wallet must be seen as an enabler. There were mixed opinions on whether the Melbourne Wallet would offer greater utility to domestic or international visitors - one participant commenting that international visitors often travel to 'cash dependent areas' e.g. Victoria market, The Great Ocean Road, where a digital wallet would offer limited value.

For security purposes the wallet could be tied to QR code rather than a personal id.

Take up could be stimulated by:

1) **Building off existing behaviour** and then modifying it
2) **Winning over an early adopter group** to drive take up and engagement. People in 30s were generally felt to be more likely to embrace it. Older people would struggle unless confident App users.
3) **Useful for international students** e.g. apply wallet allows you to pay outside country with outside card AND tap and pay option; Options to use Apps e.g. reservations through restaurants with name and phone number but not forced to subscribe to email chains; Apps useful for international students e.g. a digital wallet that allows you to pay outside country with outside card AND use a 'tap and pay' option
4) **Promotion done through social media** (Instagram, Facebook) and through a cross pollination of information across the wallet. For international visitors, this could be either promoted at the airport or via the flight crew on the incoming flight. The wallets should be available for purchase prior to arrival or at the airport. Tickets could be added via QR codes as purchased.
5) **An attractive design**: The wallet must be easy to use; offer a good overview of and clear guidance to what is available and how to access it i.e. easy to navigate. It should have good functionality and integrate easily with other key Apps e.g. Google maps, Myki, translation

Apps, banking Apps, Tripadvisor type Apps, booking Apps etc. It should be easy to set up and remove. It should offer some level of customisation in appearance e.g. by Apps; themes; age; culture; language; dietary needs; support of social causes etc. It might allow Apps to be collected into themed digital wallet containers/areas. The wallet should be subsidised (e.g. through online ads) or free and have a strong reputable promoted developer/organisation behind it.

6) **Provided security options such as facial recognition** to access the wallet; and some control over what information is tracked, collected, shared; and what suggestions are provided.

4.3 What items to include in the Melbourne wallet

Participants identified several items to be included in the Melbourne Wallet (Table 2 – next page). Items common to both international travellers and domestic residents were transport and location (e.g. Myki cards, maps), recreation (e.g. updates on events around town), and options to set language preference. Popular additional items for international travel also incorporated translators, currency convertors and trip advisors. Popular additional items form domestic users were around things that brought convenience e.g. parking availability and pay, local council information.

Table 2 shows suggested content for both domestic and international visitor usage

	Domestic	International
Driver's License	√√	
Bank	√√	√
ID	√	√√√
Credit card		√
Navigation: ***Google maps (ways to get to the city) – see also maps.me itinerary & maps; Google arts and culture; library, museums, shows, zoo***	√√	√√√√√
What's on near me: ***events, food, shopping – customised and relevant, Fun facts about Melbourne, local discounts***	√√√√√	√√√√√√
Different language mode	√√√	√√√
Translator		√√√√√
Currency convertor		√√√
Trip advisor App e.g. Restaurant App through shared partnerships *(unlikely to trust a govt App for restaurants)*		√√√√
Lonely planet/red hat/Instagram advisor type info	√	√
Accommodation details		√√
Tourist spots		√√
Health cards, and medical help	√	√
Myki/Travel card/taxi	√√√√√√	√√√√√√√√
Transport/Tram tracker		√
Pay for parking & parking availability	√√√√	
Loyalty/membership cards/partnership deals	√	√√
Coffee card	√	
Basic council information & utility companies	√√	
Local parks and gardens and utilities available	√√	
Accommodation		√
Fuel tracker		√
Access to social media		√
Recommendations on local Apps to use		√

5.0 Smart cities and the IoT

This section covered smart devices available now and participants vision of the future. Thoughts about SSI are also included in this section.

5.1 Use of voice enabled devices

There were mixed responses to using voice enabled devices (e.g. Siri, Google home devices). In line with other App usage, distinctions were made based on the value placed by the individual on the service being offered by the device. For example, some respondents were happy to use devices to remotely turn on lights or air conditioning at home (for comfort or security), to entertain or inform children or to provide company for aging parents and those with recent loss (seen as an enabler). One person would like to use voice enabled devices to learn more about own behaviours and patterns (as an informer). Others saw voice enabled devices as a 'huge invasion of privacy' with concerns about home safety due to security breaches. Finally cost was seen as a barrier to take up.

5.2 Use of digital tokens

There were mixed reviews about the use of digital tokens to hold personal information. Some felt they would increase security by having something that was discreet from view and only focused on one or two functions. Others thought it would be too easy to have it stolen or to lose it.

5.3. Using SSI to secure identity

Most participants found SSI intriguing. Some welcomed the opportunity to have verifiable key data in chunks they could control in terms of what information was shared, to whom, when and how.

> *In the future, like an electronic information repository that you're in control of your information would be great, because you would be able to say, to whatever service 'No, you don't need to know where I am when I made this decision'. (Participant 14)*

Others felt they would be unable to commit to SSI because they did not fully understand how it worked.

5.4 Vision of the future

In the future, like an electronic information repository that you're in control of your information would be great, because you would be able to say, to whatever service No, you don't need to know where I am when I made this decision (Participant 14)

It actually kind of worries me as to where else we can go? And how more linked things become and who has control of the data and most importantly, what worries me is not necessarily somebody having the data but what they use it for (Participant 13)

Participants acknowledged that life was likely to become more digitally connected and enabled and that one needed to be part of it or get left behind. Some were fascinated and enthusiastic about increased convenience whilst a few exhibited significant reluctance in moving forward. Recognised benefits were around increased convenience; connectivity; more sophisticated Apps; enhanced security; and financial and social benefits to The Public and community.

Specific examples illustrate some of these advantages. An aggregator App that pulls together and appropriately links all key Apps used in an easy to access format (e.g. Shopback). Seamless interconnections with loved ones. Cheaper data access and usage. Better algorithms to offer recommendations that added value as you moved through a Smart city – for example

1) Offering specific time constrained discounts or deals as you neared a particular location e.g. the coffee shop on the right will give you a 5% discount in the next 5 minute.
2) Increasingly streamlined payment mechanisms that would, for example automatically register an item you are carrying out of a shop and pay for it automatically.
3) A short cut key to bring up ID on things you want it to.

Increased interconnectivity and greater sharing of information naturally also raised concerns over privacy with some participants saying they would sit on the fence and wait for others to test new technologies before taking it up unless forced to take up. Concerns remained about who is accessing and controlling the data and what they would use it for. There was some concern over increased inequity and access. Increased anonymity also raised the concern that this could encourage people to behave badly because they were now non-identifiable. It was felt that an ID validates who the person is and controls poor behaviour.

Just as we behave ourselves in society, because reputation affects how we interact with society, when you take that away, people behave really badly. So I think, I think knowing people's identity is one of the key solutions to better behavior on the internet. (Participant 14)

6.0 Conclusion and Recommendations

Australia rank 8 in the provision of online services (World Bank Group, 2016) which shows Australian citizens are key embracers of digital technologies, accessing digital services at an exponential rate. However, the degree of trust in their use remains under explored within the Australian context. Our research suggests that whilst digital technologies have the potential to contribute significantly to quality of life, in the context of digital wallets and related Apps, there exists a tension between perceived benefit and risk arising from an individual's perceived social and psychological concerns. This led to a wide variance in what constituted risk. This risk appeared to be mitigated by the following factors which were identified for both general wallets and the Melbourne digital wallet:

- an Apps ability to address a perceived personal need;
- some control over privacy of personal information;
- an easy to use App design;
- an overview understanding of how the App operated on the phone and what data it accessed to operate; and
- trust in the provider's reputation.

The following recommendations would help to validate and extend existing findings.

1. **Utilise quantitative research to validate findings in the broader community.**

2. **Explore the tension between perceived benefit/risk arising from an individual's perceived social/psychological concerns as this was a key contributor to the wide variance in what constituted risk.**

3. **Explore what constitutes social risk and what this means for current and anticipated social processes in relation to the use of digital wallet and App technology as few of the participants directly considered these important aspects.**

7.0 References

The World Bank c. 2016, 'Digital Adoption Index, viewed 15 April 2020, <https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index>.

Alkhunaizan, A. and Love, S., 2012. What drives mobile commerce? An empirical evaluation of the revised UTAUT model. *International Journal of Management and Marketing Academy*, *2*(1), pp.82-99.;

Balan, R.K., Ramasubbu, N., Prakobphol, K., Christin, N. and Hong, J., 2009, June. mFerio: the design and evaluation of a peer-to-peer mobile payment system. In *Proceedings of the 7th international conference on Mobile systems, applications, and services* (pp. 291-304).;

Benson, C.C. and Loftesness, S., 2012. Interoperability in Electronic Payments: Lessons and Opportunities. *CGAP report commissioned to Glenbrook, available at: http://www. cgap. org/sites/default/files/Interoperability_in_ Electronic_Payments. pdf (accessed 15th June, 2015)*.;

Comninos, A.C., Esselaar, S., Ndiwalana, A. and Stork, C.S., 2009. Airtime to cash: unlocking the potential of Africa's mobile phones for banking the unbanked. In *IST-Africa 2009*. International Information Management Corporation Limited.

De, P., Dey, K., Mankar, V. and Mukherjea, S., 2013, October. Towards an interoperable mobile wallet service. In *2013 10th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT)* (pp. 1-6). IEEE.;

Ebringer, T., Thorne, P. and Zheng, Y., 2000. Parasitic authentication to protect your e-wallet. *Computer*, *33*(10), pp.54-60.

Ghag, O. and Hegde, S., 2012. A comprehensive study of google wallet as an NFC application. *International Journal of Computer Applications*, *58*(16).;

Houngbo, P.J., Hounsou, J.T., Damiani, E., Asal, R., Cimato, S., Frati, F. and Yeun, C.Y., 2018, May. Embedding a Digital Wallet to Pay-with-a-Selfie, from Functional Requirements to Prototype. In *International Conference on Emerging Technologies for Developing Countries* (pp. 47-56). Springer.

Houngbo, P.J., Hounsou, J.T., Damiani, E., Asal, R., Cimato, S., Frati, F. and Yeun, C.Y., 2018, May. Embedding a Digital Wallet to Pay-with-a-Selfie, from Functional Requirements to Prototype. In *International Conference on Emerging Technologies for Developing Countries* (pp. 47-56). Springer.

Neeharika, P. and Sastry, V.N., 2014. A Novel Interoperable Mobile Wallet Model with Capability Based Access Control Framework. *International Journal of Computer Science and Mobile Computing*, *3*(7).),

Ravi, N.C., Muppalaneni, N.B., Sridevi, R., Prasad, V.K., Govardhan, A. and Padma, J., 2018, December. Advanced Access Control Mechanism for Cloud Based E-wallet. In *International conference on Computer Networks, Big data and IoT* (pp. 392-399). Springer.

Rathore, H.S., 2016. Adoption of digital wallet by consumers. *BVIMSR's journal of management research*, *8*(1), p.69.

Shaghayegh, B., 2011, July. Using service oriented architecture in a new anonymous mobile payment system. In *2011 IEEE 2nd International Conference on Software Engineering and Service Science* (pp. 393-396). IEEE.,

Taghiloo, M., Agheli, M.A. and Rezaeinezhad, M.R., 2010. Mobile based secure digital wallet for peer to peer payment system. *arXiv preprint arXiv:1011.0279*.