Digital Identity: Ground-up Perspectives

Report Summary

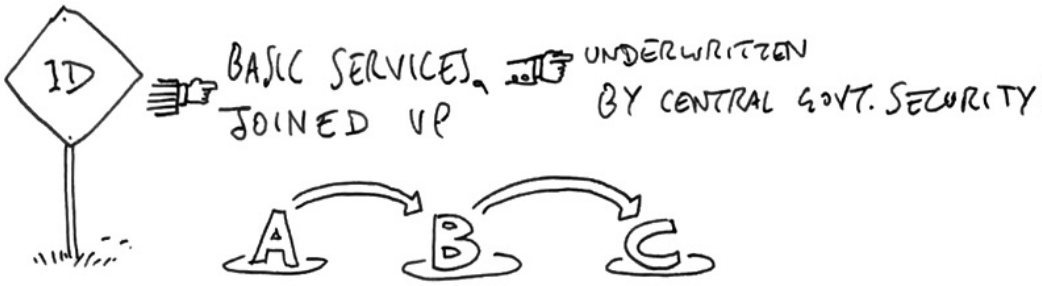
A team at Royal Holloway University of London was commissioned to run a short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of digital identity. DCMS commissioned a programme of 4 consultation sessions to be undertaken with groups who are dependent on digital identities for use with essential, core services such as finance, welfare, health, housing and education. These services may be delivered both by government and by commercial entities. Each consultation session was split into two parts: 1) Everyday experiences of digital identity and the challenges faced when managing digital identity; and 2) Requirements for future digital identity schemes.

The purpose of the consultation is to provide a snapshot of how digital identities are part of everyday lived experiences and to provide input on the design of future digital identity schemes. These consultations are part of the wider call for evidence from DCMS on the topic of digital identity. This report summary highlights the main points. Following on from the report summary, the findings are presented in the main body of the report together with the reports produced after each consultation session.

In summary, digital identity is something that people encounter in their everyday lives, most routinely so if people are dependent on essential core services for their welfare. The consultation sessions revealed that it was not uncommon for people to need help to manage their digital identities. Such help might come from professionals working in support services or from friends and family providing more informal help. From an identity service perspective, such third-party support can be regarded as a form of social proxy.

During the sessions there were frustrations expressed about the design and use of digital identities in everyday lives. In particular there were frustrations over what was required in terms of proof of identity: ***how often*** they had to prove their identity, in ***what format*** they had to provide that proof, and ***variability*** on what constitutes proof.

There were also frustrations expressed about the ***language*** used around digital identity - which was felt to be too difficult and too technical for some. This can be a problem both for native English speakers and for those for whom English is not a first language.



Report Summary

The ***cost*** of proof was too high for some: the cost of a passport or of a provisional driving licence, the cost of printing documents, the cost accessing copies of documentation such as birth certificates. The technological costs of accessing digital identity services were also too high for some: the cost of the technology needed and the cost of connectivity.

The digitalisation of services had left many feeling unsure of how to access essential services and frustrated by the ***lack of help*** and support on offer from the service providers. This lack of support left some participants describing the digital services as adversarial and a cause of great stress.

It was felt digital identity systems could also be ***too rigid*** and not have the flexibility to recognise the varied status and roles of individuals. For example, very often individuals caring for a sibling are not able to have their caring role reflected in the set-up of their sibling's digital identities.

Despite these challenges, participants recognised the value of a digital identity scheme that could be universally applied to all essential services. However, such a scheme, it was felt, would only be successful if it was designed so as to not dis-benefit people with limited capabilities and limited resources. Each participant group, in their different ways, reflected on their hopes and aspirations for future digital identity schemes. All groups coalesced around the following hopes:

A digital identity scheme that works for the people, not the people work for the digital identity scheme.

A digital identity scheme that respects a person's rights and that is accessible to all.

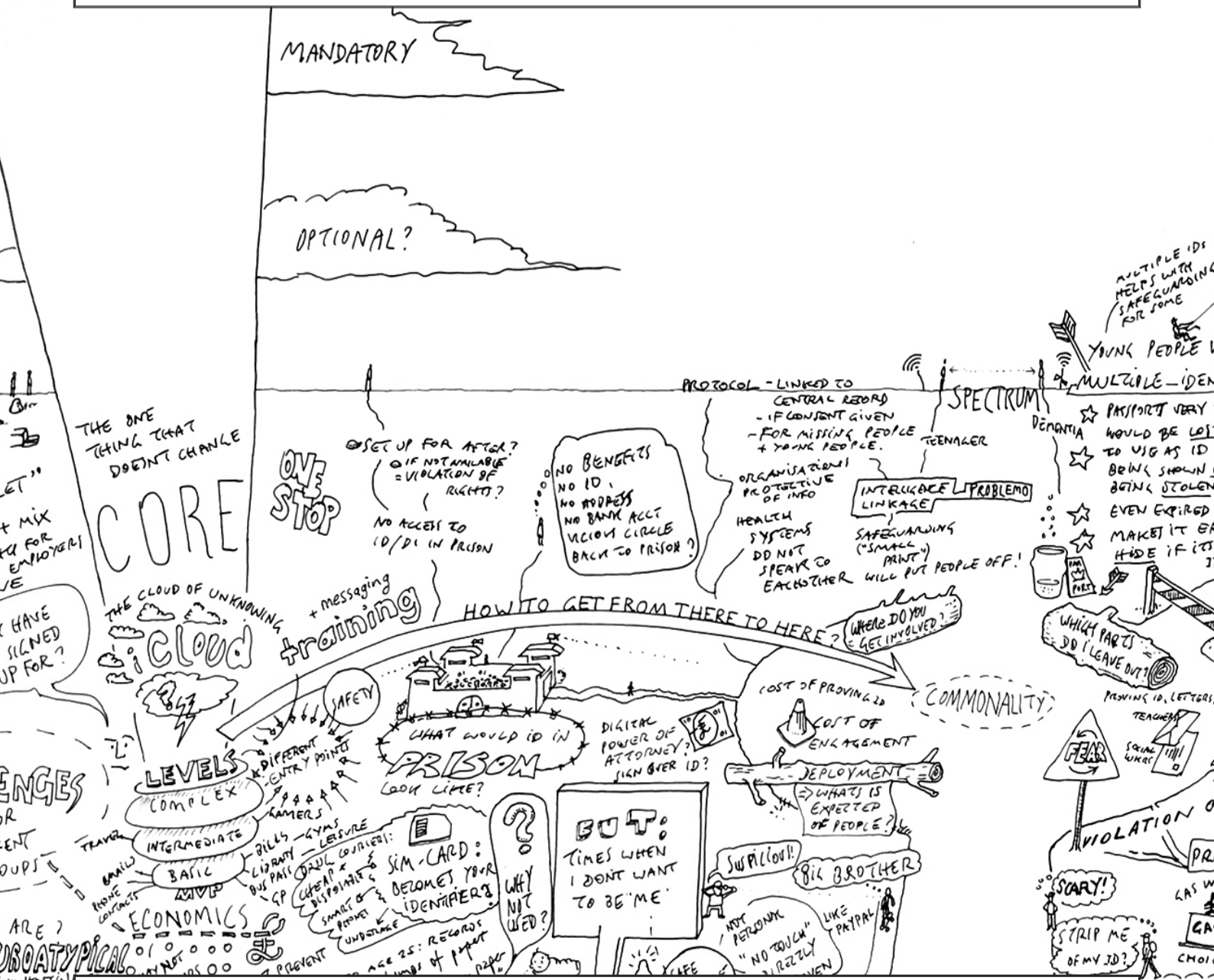
A digital identity scheme that enables a person to have autonomy and control over their own identity.

To realise such hopes, we perhaps might need to rethink how we design digital services, so that we are able to identify the relationship such services have to the roles people carry out in their everyday lives. This may result in a conceptualisation of digital identity that is not based on a single technology but, instead, ***a collection of identity tools and processes embedded within the naturally occurring support structures in people's everyday lives***, and ***over which people have both autonomy and control***. The value of such a digital identity scheme is more naturally framed by the benefits people realise from the service access that it enables, rather than solely from the efficiency gains such technology makes possible.

Due to COVID-19 restrictions, the consultation sessions were held remotely via Zoom. In order to retain the everyday detail of each session regarding the complexity of digital identity set-up and use, sketch-notes were made by Claude Heath. All the illustrations in this report are taken from the visual notes made during the consultation sessions.

DIGITAL IDENTITY

GROUND-UP PERSPECTIVES



Royal Holloway University of London
Short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of Digital Identity.
Lizzie Coles-Kemp Information Security Group
Claude Heath Department of Media Arts

September 2020

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Introduction

The Department for Digital, Culture, Media and Sport (DCMS) commissioned a programme of four consultations to be undertaken with groups who are dependent on digital identities for use of essential, core services such as finance, welfare, health, housing and education. The purpose of the consultation was to present the current lived experience of setting up and using digital identity, and to provide input on the design of future digital identity schemes; in particular, who should run them and how to make them safe, inclusive and accessible.

It was agreed that the consultation programme would not seek to be representative of society as a whole but that each consultation would provide a window into the lived experience, hopes and wishes of a specific group of people who are particularly dependent on digital identity for the accessing of core services in their everyday life. Each consultation would provide a ground-up view of digital identity, and that would be complemented by the views of the other groups over the course of the consultation programme. The views of each group are presented in their own right, and the overarching themes from across the groups are presented in the introductory sections.

A pre-consultation activity was undertaken to identify groups willing to participate and to design the format of the consultation sessions. These initial contacts made during the pre-consultation phase revealed that, while useful, digital identity is, for many, an abstract notion that is difficult to articulate. It was therefore decided that digital identity, for the purposes of the consultation programme, would be better defined as “proving who you are on-line.”

The Royal Holloway University of London team:

Lizzie Coles-Kemp and Claude Heath from Royal Holloway University of London undertook this work. Lizzie Coles-Kemp is part of Royal Holloway’s Information Security Group; she is a researcher who works with groups often regarded as marginalised or under-served, to better understand how technology can be used to improve the safety and security of such groups. Claude Heath is a researcher on the StoryFutures project at Royal Holloway’s Department of Media Arts, researching how risk can be perceptualised immersively, within the creative media industry and in wider society.

Claude and Lizzie have worked together since 2012 engaging with groups in Australia, Belgium, England and Wales to draw out the everyday experiences of interacting with digital technology and services, and to capture hopes and aspirations for secure digital futures. They produced a series of booklets on the practices of everyday security (https://bookleteer.com/collection.html?id=28) which is featured in NCSC’s You Shape Security guidance (https://www.ncsc.gov.uk/collection/you-shape-security), and a report on everyday experiences of Internet of things (IoT), as a supplement to the Secure by Design report from DCMS.

The Consultation Process

The pre-engagement phase revealed that people have rich experiences of managing digital identity in their everyday lives and that many also have strong views as to what a future digital identity scheme might look like. As a result, each consultation session was split into two parts: 1) Everyday experiences of digital identity and the challenges faced when managing digital identity 2) Requirements for future digital identity schemes.

Due to COVID restrictions, the consultation sessions were held via Zoom. Given the on-line medium and the abstract nature of the topic, it was decided that the sessions would need to be as simple as possible. The risk with running a session in this way is that the consultation might lose the details about the complexity of everyday life into which the digital identity was being set-up and managed. To offset this risk, it was agreed that one of the RHUL team, Claude Heath, would visually illustrate the session using a form of visual note-taking. Excerpts from the visual notes are used throughout the summary sections to give texture and framing to the concept of digital identity - in a bid to highlight the different and often complex ways in which digital identity is woven into everyday life. The visualisations also highlight the particularities implied by the phrase “particularly dependent on digital identity.” They show what happens when digital identity processes do not work as expected, when they are inaccessible or unusable or do not align well with the circumstances in which people find themselves using digital identity.

The session structure for each consultation was as follows:

* **Introduction** to the consultation and re-statement of consultation goals.
* **Statement** of the ethics policy and re-statement of the agreement to participate.

There then followed a semi-structured group discussion using the following discussion prompts:

1. Explain specific **examples** of digital identity, where you have supported people to apply for a digital identity and the barriers and challenges that have arisen.
2. Run through additional **scenarios** of where digital identity might be used.
3. Discuss the **potential benefits and challenges** of having one digital identity.

Once each session was completed, notes were written up and sent back to the session’s participants for comments and review. The session notes were then turned into a report. The consultation reports can be found at the end of this report.

Recruitment and Participants

Participants were recruited through an existing community group network. Lizzie Coles-Kemp has worked with community groups across the UK since 2008 on the topic of digital participation and digital safety and security. Through her network, she recruited groups who are particularly dependent on digital identity schemes for access to essential services. The small size of the consultation programme means that the results from this consultation programme cannot be regarded as representative of UK society as a whole. However, participation in the 4 consultation sessions were recruited in such a way that there is a representation of a wide range of dependencies on digital identity and on essential service providers from the public and private sectors. The groups also represent a range of socio-economic contexts.

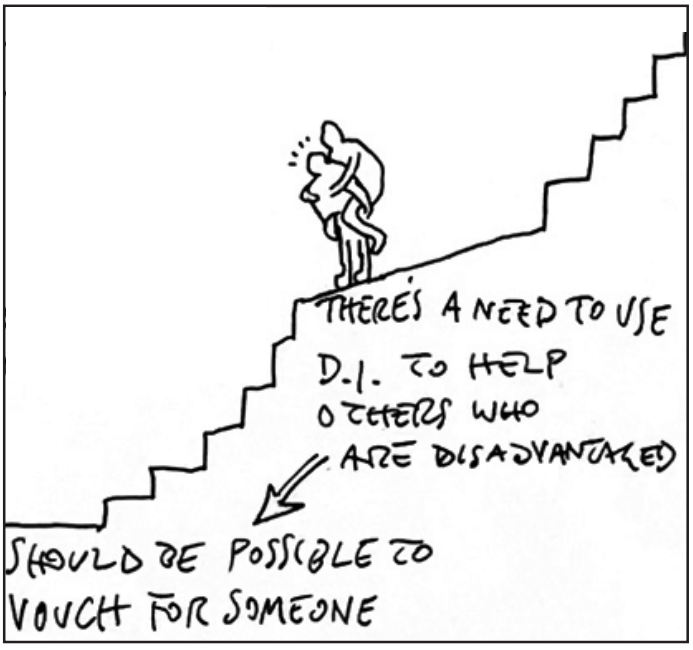
The following groups took part in this consultation programme in five consultation sessions:

1. **Matthew's Hub**: a third sector organisation that supports vulnerable neuro-diverse people from aged 13 to 70+.
2. **Cornerhouse** (Yorkshire): an organisation supporting children and young people with a focus on emotional and sexual health and wellbeing.
3. **North Bank Forum**: is a voluntary and community sector umbrella organisation based in Hull and operating across Yorkshire and the Humber.
4. **Sibs**: a charity supporting those with siblings who are disabled.
5. **CIAC**: a registered charity that supports emerging communities to contribute fully to life in the UK as committed and active citizens.
6. **Intergenerational Group** of four participants, who between them represented all the dependencies on digital identity that were identified across the other five groups.

Groups 1-3 are reported in the report titled 'Hull's Voluntary and Community Report', while the other groups have their own separate reports.

All participation took place following the research ethics policy at Royal Holloway University of London.

Consent was confirmed at the start of each consultation session and was re-confirmed again as part of the report writing stage. The reports from each session are included in the overall report with permission. All illustrations are published under a Creative Commons licence and are owned by Claude Heath.



Everyday Experiences of Digital Identity

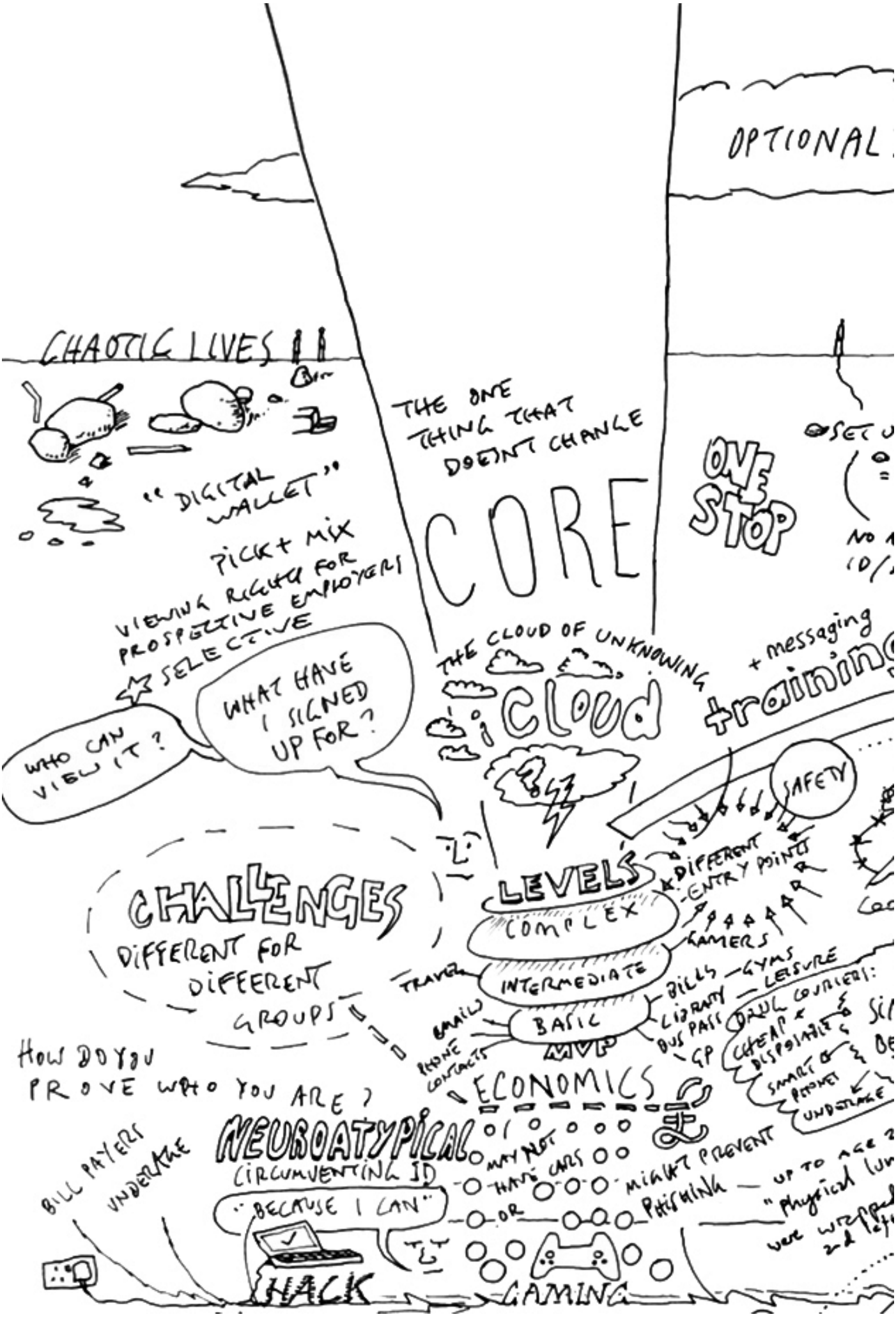
Across the participant groups, the main contexts in which digital identity currently occurs are: set-up and use of a bank account, book a doctor's appointment, order prescribed medicine, claim welfare, apply and pay for housing or apply for a grant or a loan. The main criticism of digital identity in all these contexts boiled down to the observation that *digital identity and the uses of such identities are designed for a particular profile of technology user.* For those who fall outside of that profile digital identity is not a benefit but a **hurdle** to be overcome to gain access to the services that are essential in everyday life.

The sessions showed that digital identity only "makes sense" when it is discussed in terms of what a digital identity can "do" for an individual. Whilst the process of setting up a digital identity is a bureaucratic activity in its own right, the majority of the discussions revolved around digital identity in use. A digital identity is used to enable a person to gain access to a service where gaining access was talked about in terms of the benefits that were realised through access. From the perspective of the participants there were three main digital identity processes at work: (1). Verifying an individual's identity in order to set-up a digital identity; (2). Gaining access to a service; (3). Finding ways to overcome the obstacles posed by a digital identity.

Verification of an individual's identity - digital identity set-up:

Many of the challenges that participants experienced when setting up a digital identity to be used with core (essential) services relate to having the necessary evidence for verification. In every session, the challenges of not having the correct records in the right format were a feature of every discussion about everyday experiences of digital identity. Another challenge experienced by participants related to the costs associated with acquiring formal documentation and the challenges of keeping that documentation to hand. Many of the participants cared for people who have complex lives and limited resources and capabilities with which to manage identity documentation.

Participants raised the problem of navigating the on-line processes through which to undertake identity verification. The language used by such services was too unfamiliar for many and the requirements and verification policies often seemed conflicting and unnecessarily complex. In addition, the design of the technological services was often not sufficiently robust, or sufficiently easy to use, and as a result it was often difficult for people to complete the verification process. Verification processes typically require a particular sequencing of tasks that can be difficult for people to grasp and are particularly difficult to complete when an individual is unconfident or under pressure. In the first two sessions, it was highlighted that verification processes can also be challenging for neuro-diverse people who struggle to follow the sequencing of identity verification tasks.


CHAOTIC LIVES
"DIGITAL WALLET"
PICK + MIX
VIEWING RIGHTS FOR PROSPECTIVE EMPLOYERS
SELECTIVE
WHO CAN VIEW IT?
WHAT HAVE I SIGNED UP FOR?
THE ONE THING THAT DOESN'T CHANGE
CORE
THE CLOUD OF UNKNOWING
iCloud
ONE STOP
OPTIONAL
+ messaging
+ training
SAFETY
CHALLENGES
DIFFERENT FOR DIFFERENT GROUPS
LEVELS
COMPLEX
INTERMEDIATE
BASIC
MVP
DIFFERENT ENTRY POINTS
GAMERS
TRAVEL
EMAIL
PHONE CONTACTS
BILLS — GYMS
LIBRARY — LEISURE
BUS PASS
GP
HOW DO YOU PROVE WHO YOU ARE?
BILL PAYERS
UNDERAGE
NEURODIVERGENT
CIRCUMVENTING ID
"BECAUSE I CAN"
HACK
ECONOMICS
MAY NOT
HAVE CARS
OR
MIGHT PREVENT
PHISHING
GAMING
SMART
PHONE
UNDERAGE
"Physical

Everyday Experiences of Digital Identity

Participants were at pains to point out that different people experience different challenges when setting up and managing a digital identity and that these challenges often combined to make certain aspects of identity set-up and management particularly difficult. Examples were given of where young people, particularly those in care or those with little access to parental support, might struggle to prove their identity because they do not have access to the necessary paperwork. In such cases young people needed to arrange for people to vouch for them, which can be complex to arrange. Further examples were given of how elderly people may not have access to proof of identity (in comparison to a person who is of working age) due to the fact that a person's need for a driver's licence and passport can decline as they get older and as their children take over the management of bills and other financial matters.

In each session, many examples were given of where the verification process had failed and how, at that point, the digitalisation of services meant that there was **nowhere to obtain help**. Each consultation group revealed that it is not uncommon for someone to help another person with their identity management activities - either as an act of support and friendship, or in a role of caring or as part of a job. Often such support could be seen as a **shared model of care** - whether formal or informal. The community and voluntary sector groups who took part in this consultation programme often gave examples of providing support for people to set up and manage digital identities via an intermediary - such as a friend or family member.

Once an identity is set-up, further challenges were experienced when trying to keep that identity safe; particularly when people are using a **shared device**, have limited access to a computer or a phone, or keeping paper copies of identity details.

Gaining access to a service:

For each participant group, gaining access to a service using a digital identity was talked about in terms of realising the benefits of a service, and not in terms of the steps taken to access a service. For example, the aim of accessing on-line banking is to be able to manage money, and to make and receive payments. Online banking and the role of digital identities were therefore most often talked about in terms of what the digital identity was used for. The value of a digital identity was measured in terms of the degree to which that identity facilitated the gaining of access. Examples were given in every session of where a digital identity did not result in service access being acheived, and the stress that ensued as a result of being denied access. For example, for some participants whilst the NHS number that each British citizen has is a clear example of a unique identifier, it does not, on its own, grant access to health services. It was felt by some that the problem of health service access is exacerbated by the introduction of digital health services as the relevant health information about a person is not necessarily made available through an individual's NHS number. This is information


WHAT WOULD ID IN PRISON LOOK LIKE?
DIGITAL POWER OF ATTORNEY? SIGN OVER ID?
DEPLOY
BUT: TIMES WHEN I DONT WANT TO BE "ME"
SUSPICIOUS!
SIM-CARD: BECOMES YOUR IDENTIFIER?
WHY NOT USED?
FROM BIRTH
NHS NUMBER
SAFE
SAFE MIDDLE PERSON
"NO TOUCH" DIRECTLY PRE-PROVEN
MATTHEWS HUB
DRIVING LICENCE
PASSPORT
BANKING
PRESCRIPTIONS
GP
THIS IS "me"
HOW YOU GET IN
PAYPAL
Passwords always get LOST!!
LOTS OF PEOPLE WHO WANT TO SPEAK TO DWP
ADVERTS APPEAR
"YES"
DWP
M·Hub
HOW DOES THIS EVEN HAPPEN?
ACCEPTED FORM OF INFO GIVING..... BUT FEELS LIKE IT COULD BE ANYONE ....
NOT TRANSPARENT
EMPLOYABILITY IN U.K
HOUSING REFERENCE
DWP
DATA
GDPR
AGREE: STAY MEMBER
RETURN: ONLY IF THEY NEED INFO + HELP
SAFEGUARDING
BE BUILT UPON — MIGHT BE EDITABLE TO PEOPLE
HOW WOULD YOU ASK FOR HELP?
CONSENT GIVEN. ⇒ HELP NEEDED. ⇒ CAN'T ACCESS IN ANY OTHER WAY...
POLICE? IS IT ILLEGAL? EVEN

that participants argued should already be on the system and identifiable through an individual's NHS number.

Digital identities that are not designed to support contexts of use therefore become a hurdle that has to be overcome in order to gain access to a service that is needed. This often leaves residual security worries and concerns when people are using a digital identity. These include:

Who can view my identity?
Who can view what I do with my identity?
What have I signed up for?
Whom can I ask for help?

Finding ways to overcome obstacles posed by a digital identity:

The sessions revealed that digital identities are not always a perfect fit for everyday life, a life that is often messy and does not fit neatly into the pre-set patterns of practice that digital services are designed to expect. The mismatch often boils down to the fact that digital services are built upon a model of a particular social structure that is often too narrowly defined. When people are in circumstances or operating in such a way that does not fit the expected social structure, problems can occur with accessing services using a digital identity. An example was given of the difficulty of managing two bank accounts (an individual's account and the account of someone they look after) at the same bank from one mobile phone. This was due to the two-factor authentication for the access control process not being designed to recognise this as a legitimate access scenario.

Digital identities in current use are not typically designed to be shared or to be used by a third party - and yet this was a frequently occurring scenario described in all of the consultation sessions. The lack of flexibility of systems in recognising different social structures partly stems from the design of the technology, but more fundamentally can be traced back to ambiguities in the underlying policy and regulation. For example, those caring for a disabled brother or sister very often found that their role as a social proxy managing digital identity and digital service access on behalf of their brother or sister was not recognised - or only partially recognised. The initial ambiguity stems from grey areas in the rules relating to power of attorney and the interpretation of capacity. This ambiguity means that there is limited provision for the social proxy role in the digital identity and service design, and as a result, the actions of a social proxy can be misinterpreted under anti-money laundering rules or under anti-terrorism rules. This makes it very difficult for someone to manage a bank account, claim welfare, or manage housing on behalf of their disabled brother or sister.

Security Risks

Essential core services in health, banking, welfare and housing are central to an individual's security and safety. They keep people safe and provide a platform from which people can safely and securely contribute to society. All our participants reflected upon how such core services were becoming increasingly digitalised, and that they increasingly required the use of digital identities. When digital identities were lost or were found to be difficult to set-up, many examples were given of where people felt pushed into potentially risky behaviours and compromising situations as a result of this difficulty. For example, people might turn to a friend or to family member to informally carry out identity set-up and management tasks on their behalf. This happens the world over: sometimes the reasons are cultural, sometimes it is because of the dynamics within a family set-up; sometimes it is because the process is too complex or the language too unfamiliar, or because there is little or no access to the technical or connectivity resources that are necessary. In many cases it is because an individual lacks the confidence to engage with the bureaucratic system and decides that relying on a trusted friend or family member feels like a safer option for them.

Whilst allowing an informal third party to act as a social proxy when setting up and managing a digital identity is usually against the policies of digital identity use, it is nevertheless seen by some as a relatively safe way to proceed. Participants gave clear examples of where people are left vulnerable if they have to manage digital identities on their own. For example, older people were felt to be particularly vulnerable to being scammed. Examples were also given of where people go without essential services because they are unable to set up and manage a digital identity. Whilst being a social proxy is often a supportive act, it puts the legal owner of the identity into a vulnerable position in cases where things go wrong with the management of the digital identity: either because the social proxy does not fully complete the tasks, or completes them incorrectly, or because the social proxy loses or does not look after the personal data that has been handed over. In addition, the social proxy might be malicious and use someone else's personal data for fraud. It also potentially puts the social proxy in a vulnerable position, because they might be open to accusations of fraud that they can't disprove, even if not true.

Here the security problem is clear: for some the involvement of an informal third party results in manipulation, while for others the involvement of an informal third party offers access to a form of control and autonomy that an individual does not have if they try to manage a digital identity by themselves. To date, security technologies often struggle to differentiate between these two scenarios, and in the meantime people find themselves taking up risky and informal identity management practices for which they are afforded little protection.

Poor choices in service design or a failure to resolve ambiguities or tensions in underlying policies and procedures can exacerbate these tensions and push people towards these riskier situations. One of the core failures in design, from the perspective

of the participants, was the lack of available support while using the digital processes and identity systems, and moreover, a lack of support when things do indeed go wrong. Time and again participants emphasised the importance of being able to **talk to someone**. It was strongly argued that better designed digital systems and the provision of support that was usable and helpful would reduce security risks of scamming or inadequate support from a social proxy.

Digital Identity - Futures

All the participants could see the potential benefits of a universal digital identity scheme, but all participants were very aware of the dangers and concerned about further loss of autonomy and control. In the current situation, there are many problems with digital identity systems. Resolving these problems in such a way that access to essential services was improved and made more effective, would be welcome for many.

When the groups talked about digital identity futures, they talked about it in one of two ways: principles and implementation.

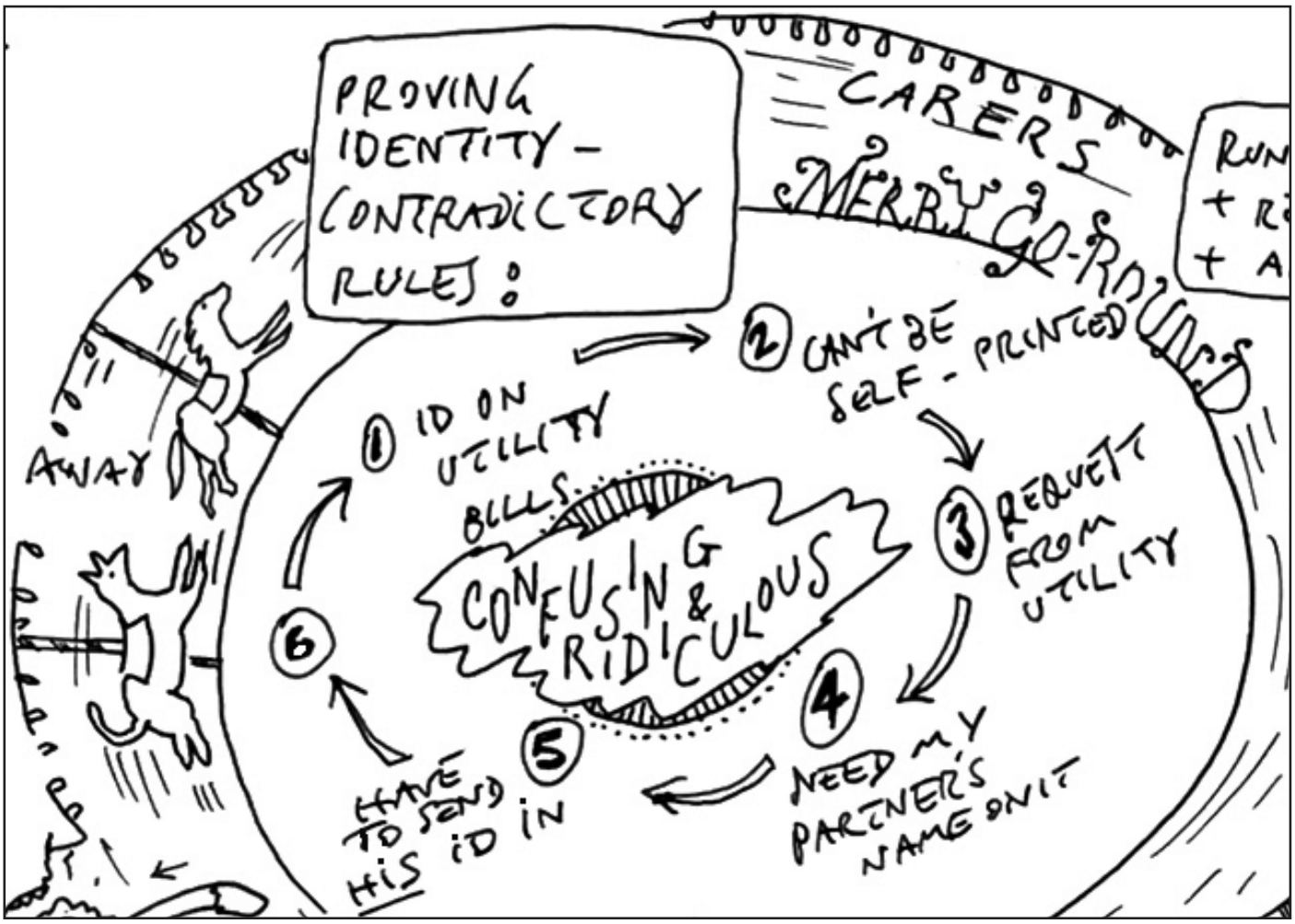
Principles:

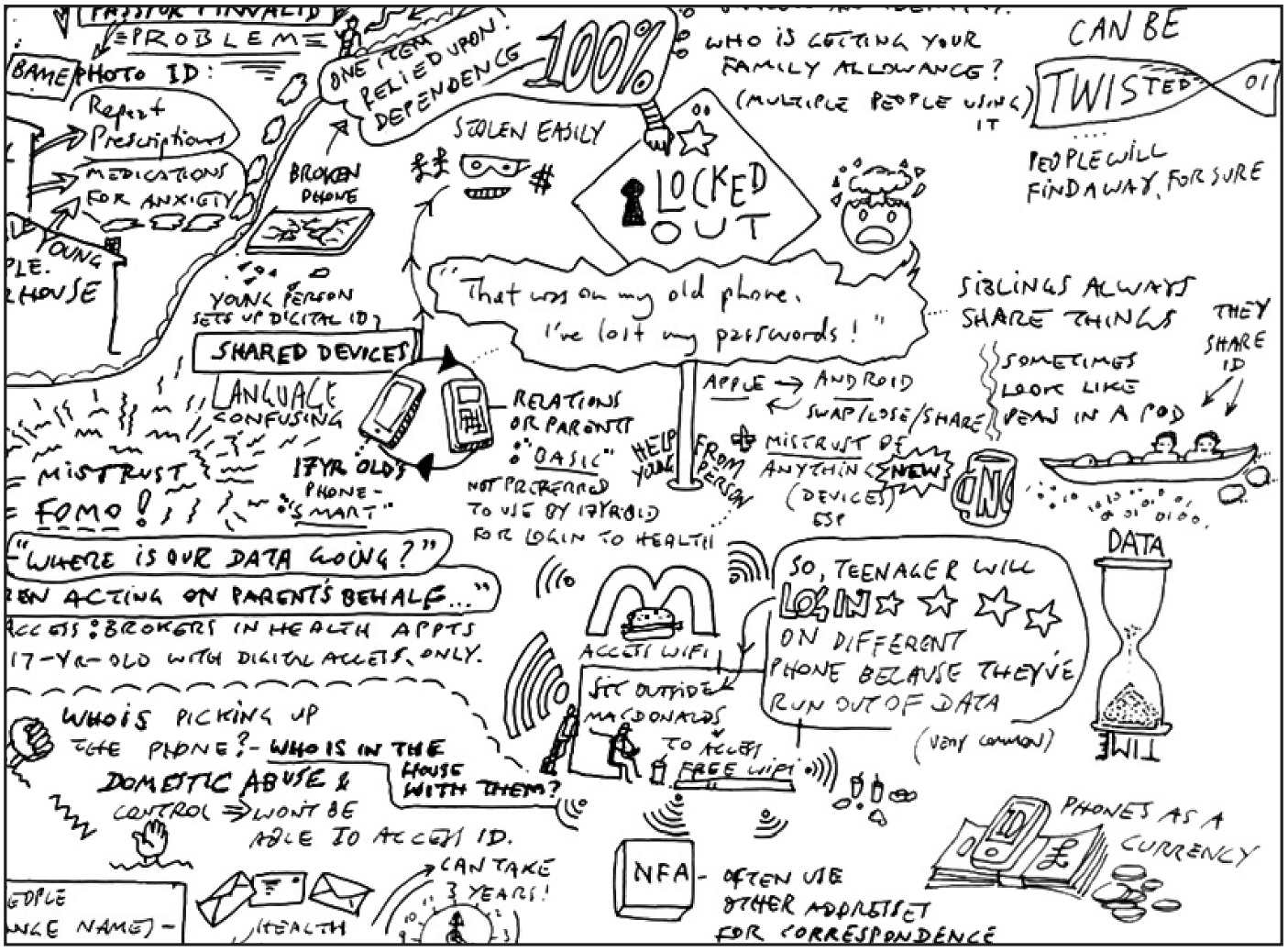
- Identity services must be **transparent**.
- The eligibility rules for a digital identity must be **clear and fair**.
- There must be clear **accountability** for the digital identity scheme.
- If it goes wrong or problems occur, it must be clear whose responsibility it is to **fix** the system.
- An identity scheme must not be imposed on people but only rolled out by **consent**.

Implementation:

- The design of the digital identity scheme must be **co-designed** with as diverse a group across society as possible. This includes the processes of governance and accountability.
- An identity must be **reliable**, consistent and usable by a wide cross-section of society.
- The rules of data use must be **clear, transparent** and fair, and support the rights of the individual.
- A digital identity system must be **secure**.
- Effective **help** must be available if users of a digital identity system encounter problems.

Two of the consultation sessions explored the idea of a **modular digital identity scheme**. This has basic digital identity services for all at its core but allows for additional identity services on top that could be adopted by those in society who need them.


PROVING IDENTITY - CONTRADICTORY RULES:
CARERS MERRY GO-ROUND
AWAY
1 ID ON UTILITY BILLS
2 CAN'T BE SELF-PRINTED
3 REQUEST FROM UTILITY
4 NEED MY PARTNER'S NAME ON IT
5 HAVE TO SEND HIS ID IN
6
CONFUSING & RIDICULOUS


PROBLEM
NAME/PHOTO ID:
Repeat Prescriptions
MEDICATIONS FOR ANXIETY
BROKEN PHONE
ONE ITEM RELIED UPON: DEPENDENCE
100%
STOLEN EASILY
LOCKED OUT
WHO IS GETTING YOUR FAMILY ALLOWANCE? (MULTIPLE PEOPLE USING IT)
CAN BE TWISTED OR
PEOPLE WILL FIND A WAY, FOR SURE
"That was on my old phone, I've lost my passwords!"
SIBLINGS ALWAYS SHARE THINGS
SOMETIMES LOOK LIKE PEAS IN A POD
THEY SHARE ID
SHARED DEVICES
YOUNG PERSON SETS UP DIGITAL ID
LANGUAGE CONFUSING
MISTRUST
FOMO!
17YR OLDS PHONE - "SMART"
RELATIONS OR PARENTS "BASIC" NOT PREFERRED TO USE BY 17YR OLD FOR LOGIN TO HEALTH
APPLE → ANDROID
SWAP/LOSE/SHARE
MISTRUST OF ANYTHING NEW (DEVICES) ESP
HELP YOUR FROM PERSON
"WHERE IS OUR DATA GOING?"
"EEN ACTING ON PARENTS BEHALF..."
ACCESS: BROKERS IN HEALTH APPTS
17-YR-OLD WITH DIGITAL ACCESS ONLY.
ACCESS WIFI
SEE OUTSIDE MACDONALDS
TO ACCESS FREE WIFI
SO, TEENAGER WILL LOG IN ON DIFFERENT PHONE BECAUSE THEY'VE RUN OUT OF DATA (VERY COMMON)
DATA
TIME
WHO IS PICKING UP THE PHONE? - WHO IS IN THE HOUSE WITH THEM?
DOMESTIC ABUSE & CONTROL ⇒ WON'T BE ABLE TO ACCESS ID.
CAN TAKE 3 YEARS!
HEALTH
NFA - OFTEN USE OTHER ADDRESSES FOR CORRESPONDENCE
PHONES AS A CURRENCY

Concluding Comments

During the study's preparation phase, the pre-study feedback clearly showed that people largely find digital identity to be a concept that is difficult to relate to and hard to define. During the consultation sessions it emerged that people have strong feelings about digital identity, the role it plays in their lives, and the hopes and aspirations that they have for future digital identity schemes. This was often a surprise to the participants, many of whom had not previously reflected on the role of digital identity in their everyday lives. However, these feelings only emerged when people talked about digital identity in the context of their everyday lives, and in the contexts of the purposes for which it is used.

The groups that took part in the consultation programme all relied on digital identities to receive services that are essential to their everyday lives and/or to the lives of people to whom they provided community and support services. Having established that digital identity is an important issue, participants systematically worked through the different examples of digital identity that they have experienced as part of access to essential, core services, examining in some detail the barriers and challenges that they encountered in the current state of affairs.

Perhaps as a consequence of this reflection, participants went on to consider what a future digital identity scheme might look like - and to suggest principles on which such a scheme might be founded. In this part of the session, each group, in their different ways, reflected on their hopes and aspirations for future digital identity systems. All groups coalesced around the following hopes:

A digital identity scheme that works for the people, not the people work for the digital identity scheme.

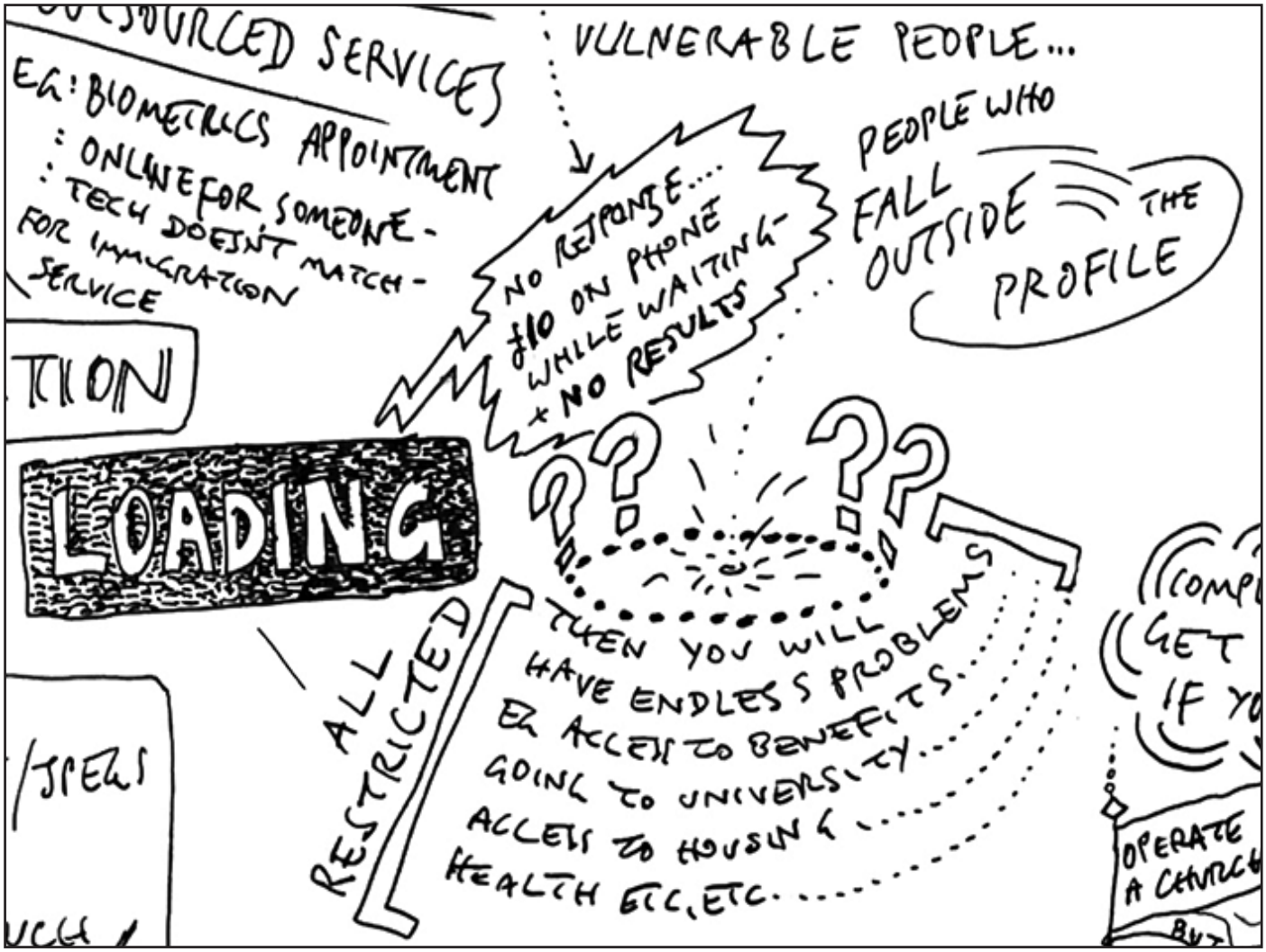
A digital identity scheme that respects a person's rights and that is accessible to all.

A digital identity scheme that enables a person to have autonomy and control over their own identity.

Whilst privacy was not directly discussed by the groups, the need for a person to have autonomy and control over their own identity was discussed. The discussions circled the question of who or what has access to an identity, and who has access to the information generated from it. This question has a direct bearing on the desire that participants have for autonomy and control, as they envisaged it in a future digital identity scheme. Their future of digital identity implies autonomy and control, and privacy stemming from the use of the future digital identity.

Concluding Comments

For these hopes and aspirations to be realised, digital identity needs to be understood not solely as a piece of technology but as a toolkit of technologies and processes that are designed for a wide spectrum of capabilities. There must also be an acknowledgement that many groups and individuals find themselves with limited resources to successfully use digital systems. It is also important that any future digital identity scheme is designed *with* (rather than for) as broad a cross-section of society as possible. By co-designing digital identity in this way, it will become apparent that a usable system means different things to different parts of society, and that a combination of good digital design and accessible in-person support will increase the likelihood that a digital identity scheme will be successful.



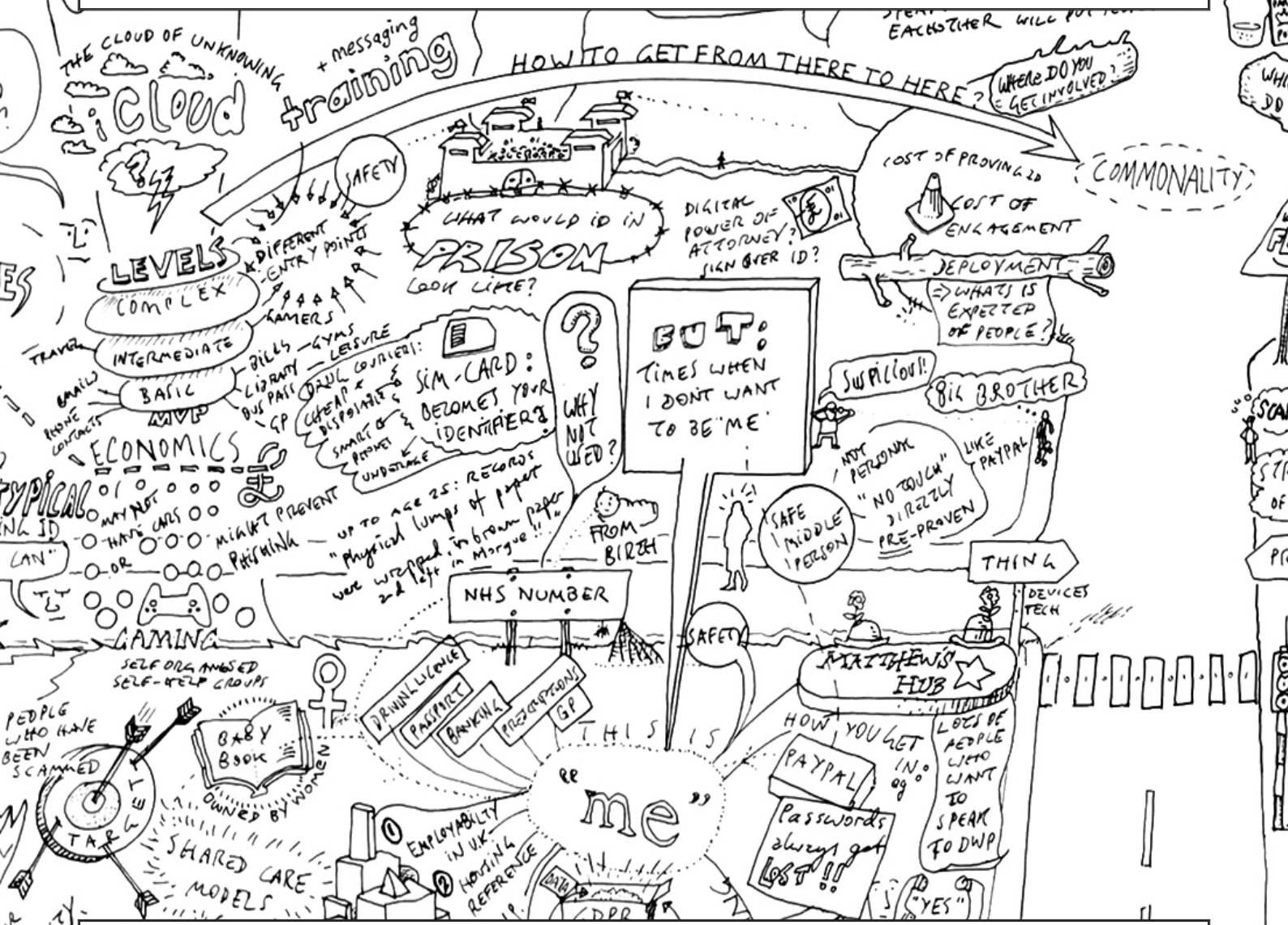

SPECTRUMS
TEENAGER
DEMENTIA
PROBLEMO
PEOPLE OFF!
PASSPORTS VERY VALUABLE & EXPENSIVE.
WOULD BE LOST BY TEENAGER - TO USE AS ID; PASSPORTS BEING SHOWN IN THE BAR + BEING STOLEN
VERY COMMON!
EVEN EXPIRED ONES USED.
MAKE IT EASIER TO HIDE IF ITS DIGITAL ID
YOUNG PERSO COMING FROM BIRTH CERTIF
COMPUTE
PASSPORT = PROB
PHOTO ID
Repeat Prescription
MEDICATION FOR ANXIE
PRIMARY CARE.
BAME
WHICH PARTS DO I LEAVE OUT?
NORTHBANK FORUM
VULNERABLE YOUNG PEOPLE.
CORNERHOUSE
COMMONALITY
PROVING ID, LETTERS:
TEACHERS
SOCIAL WORK
FEAR
VIOLATION OF ME
MISTRUST
FOMO!
PRIMARY CARE
"WHERE IS OUR
CHILDREN ACTING ON
SCARY!
GAS WINS!!
GAS
WIFI
CHOICE
ACCESS: BROKER
JUST 17-YR-OLD WITH
STRIP ME OF MY ID?


"YOUR CALL IS IMPORTANT TO US..."
CHAT BOTS - NO LIVE PEOPLE!!

DIGITAL IDENTITY

GROUND-UP PERSPECTIVES

Hull's Voluntary and Community Sector



Royal Holloway University of London
Short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of Digital Identity.
Lizzie Coles-Kemp Information Security Group
Claude Heath Department of Media Arts

September 2020

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Introduction -
Hull's Voluntary and Community Sector

A team at Royal Holloway University of London was commissioned to run a short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of digital identity. DCMS commissioned a programme of 4 consultation sessions to be undertaken with groups who are dependent on digital identities for use with essential, core services such as finance, welfare, health, housing and education. The purpose of the consultation was to provide input on the design of future digital identity schemes; in particular, who should run them and how to make them safe, inclusive and accessible. These consultations are part of a wider call by DCMS for evidence on the topic of digital identity.

Each consultation session was split into two parts: (1). Everyday experiences of digital identity and the challenges faced when managing digital identity, and (2). Requirements for future digital identity schemes.

Due to COVID restrictions, the consultation sessions were held via Zoom. In order to retain the details about the complexity of digital identity set-up and use in everyday life, Claude Heath visually illustrated the session using visual note-taking.

Participants: Hull's Voluntary and Community Sector

This report is the product of two consultations that took place with representatives from the following third sector groups in Hull: Matthew's Hub, North Bank Forum and Cornerhouse.

Two representatives from **Matthew's Hub**: one speaking in her capacity as lead for Matthew's Hub and from a background in healthcare and safeguarding and one in her capacity of service manager at Matthew's Hub. Matthew's Hub is a third sector organisation that supports vulnerable neuro-diverse people from aged 13 to 70+.

One representative from **North Bank Forum** speaking from both the perspective of primary care and BAME support. North Bank Forum is a voluntary and community sector umbrella organisation based in Hull and operating across Yorkshire and the Humber.

One representative from **Cornerhouse (Yorkshire)** is an organisation supporting children and young people with a focus on emotional and sexual health and wellbeing.

The views expressed are those of this participant group.

Everyday Experiences of Digital Identity - Hull's Voluntary and Community Sector

Much of the work of all three organisations is to advocate and to facilitate access to core services on behalf of other people. Digital identity management can be a part of that work, particularly in respect to setting up access to digital services for welfare, banking and housing. For example, Matthew's Hub currently has circa 800 contacts per week (not necessarily from different people but 800 calls that require follow-up or action). A lot of the work generated by these calls is to help neuro-diverse adults navigate core services.

North Bank Forum highlighted how digital identity is often a core aspect of access to primary care. For example, to get repeat prescriptions you have to prove who you are. In particular, not having a driving licence or passport (Photo ID) is a problem. If someone is struggling with anxiety, this challenge can make them more anxious. In everyday digital identity management there is a fear about where the information is going as well as a fear of missing out if you don't have a digital identity and access.

Within families, the need to access digital services can mean that you are relying on a young person to help you set-up and use a digital identity. Shared access may take place because older members in a household have simpler phones with less access to data. Shared access may be problematic if the younger person is not willing to share their data. This manner of shared access can also be a problem for healthcare because there may be things that the older members of the household does not want to share with a younger person in a family. In addition, the language that is used in digital access can be complicated or confusing and this can be made worse when the older person has to go through a young person as a third party.

The above problems are also seen by youth services when they are advocating on behalf of a young person: Having the right information to prove who you are as a young person (particularly if you have been through the care system) can be problematic and there can be a delay in getting access to information because you cannot prove who you are. Examples were given of having to find ways round no photo id for young people or young people not having a birth certificate. This would include sourcing letters needed from social workers and/or teachers.

Across all three organisations, the digital identity challenges experienced by their communities come from several sources: insufficient access to technology, data and internet; difficulties in understanding how to navigate the services and what data is required; lack of access to the right paperwork and proof of identity.

Representatives from Matthew's Hub highlighted that their members consult them about access to core services but not to services such as gaming and other less formal services. It was felt that gaming is a grey zone where people might actively avoid the use of a central, government sanctioned identity. Gaming also introduces the notion of multiple identities and for some people multiple identities help with safeguarding by enabling them to control who they come into contact with and when. In the digital realm, there are many examples of where young people choose another

identity and they want to be recognised for that new identity. Young people also have multiple identities on-line and they want to be able to inhabit those different identities.

Digital identity is used by some more than others which means some encounter more hurdles to using digital identity than others, it was argued. In the case of healthcare, more frequent and routine use of digital identity is part of some health conditions. For example, if you have diabetes, you might have to re-new your driving licence every three years which is now typically carried out on-line and is complicated to do without a passport to verify who you are.

All three organisations concurred that the requirements for proving you are who you say you are often have economic costs (cost of a passport, driving licence and replacement birth certificate). It can often include the economic cost of needing to have a fixed abode through the requirement of proving the address of your accommodation. They also require that you have to know how to navigate identity services and understand what they mean. For groups with low levels of literacy, low levels of confidence and who are experiencing high levels of stress, navigation of such services might be difficult.

The consultation group saw the dependence on digital technology as a barrier to using digital identities. If technology is to be used to prove who you are, there is the potential for people to become too dependent on the technology and this is a problem if the technology fails. If people have to be dependent on technology, they may feel that big brother is watching and that it is a form of control, with the result that they won't use it.

The three organisations represent a broad spectrum of groups and communities. During the session they frequently gave examples of what constitutes unreasonable third party use of digital identity is different for different people. The group highlighted that whilst the barriers and challenges to accessing and using digital identities look different to different people, the cause and effect are the same (e.g; socioeconomic barriers). Proving your identity can involve so many peripherals (for example passport, smartphone) and these all have costs associated with them which can act as a barrier for many groups. It was also pointed out that mobile phones are a form of currency and can be bought and sold at the end of the month to pay bills; a high-tech phone carrying ID also becomes a prime target for theft.

Digital identity also assumes digital access; families and individuals do not always have access to the internet. Even if there is a WIFI service, the access can change from week to week; for some it comes down to a choice between paying for gas (for cooking and heating) or wifi and gas will usually win.

It was agreed that introducing a digital identity scheme will be difficult because there is always a mistrust of anything new and there is always worry that the information will not get to the right people. The participants outlined some of the challenges for a future scheme.

Future Digital Identity Scheme - Hull's Voluntary and Community Sector

Challenges:

The group felt that having a single digital identity when it works would be amazing but very problematic when it doesn't work.

One of the key challenges is who owns and manages the identity. In some of the participants' experience, many of the problems come when people do not own or control their own identifiers. An example of the power of controlling your identity can be found in maternity care where the women undergoing pre-natal care control their own identity and the data associated with it.

Another challenge is differentiating between legitimate and illegitimate use of an identity; an identity is something that can be used to hide behind and there is the potential for someone's digital identity to be used for another person's gain. For example, one person's digital identity can be used by another to gain access to someone else, to generate debt in someone else's name as a form of coercion, or to commit other forms of domestic abuse.

The cost of accidental loss is also a challenge. Having a formal form of digital identity could be expensive and the cost if you lose it is significant. Having a formal digital identity also makes you a target of theft. The cost of an identity is only worth it if a). the checking of the identity is robust and fair b). you get something worth having in return for having the digital identity. There also has to be a robust way to retrieve a digital identity if it is lost.

Another challenge is designing processes that meaningfully use digital identity in an inclusive way. It is not just about the digitial technology but that also that the processes for using the identity technology have to be clear and understandable. If you make the digital identity scheme technology-based (e.g. store it in a phone or an app on a phone) then it has to work for all as people can feel unfairly victimised if they are not included.

A further challenge is ensuring that the digital identity has meaningful value. The value of the identity is what you have access to. Identity is not separate to the information that you have access to. Therefore: technology needs to be well-designed (i.e. integrated with the services that support it), trustworthy, secure (so that you can guarantee that the digital identity belongs to the person using that identity) and needs to give confidence that the information that the digital identity is used to access is not shared with others without permission.

Finally, people's relationship to the digital identity scheme has to be healthy. A single digital identity might also be seen as a target, simply 'because it is there', and 'because I can', and because hacking it is a challenge. As a society, our relationship with digital identity has to be re-worked so it is not seen as fair game but seen as fair and a valid resource for all.

Future Digital Identity Scheme - Hull's Voluntary and Community Sector

Support:

The three organisations provide support services to individuals and their families from many backgrounds. They argued that the success of a digital identity scheme would hinge on support from such organisations. In particular, the messaging would need to be clear and the benefits would have to be precisely and simply articulated. It was highlighted that it would also be important to set up support (local as well as central) and provide clear messaging to stop people being scammed.

Support from the Voluntary and Community Sector is important if non-compliance and misuse of a future digital identity scheme is to be reduced. It was acknowledged by the participants that some people will always try to twist the scheme/hack technology. If the digital identity scheme is mandatory and universal – some will always try to hack it. However, some of that risk can be reduced with education, messaging and ensuring that there is genuine benefit to using the technology.

The digital identity scheme and services must be simple and clear to use, not be dependent on particular technologies or on other people.

Possible Future Schemes:

All participants agreed that a digital identity scheme that removed a lot of the current challenges would be beneficial. The participants suggested a multi-layer or modular digital identity which started as a core identity that provided access to essential services. Each additional layer of the identity might offer a greater level of functionality but would also be more complex to manage. Those who need simple access to only a few core services would have a simpler identity to manage, this would mean less bureaucracy. Examples of core services would be bill payment, library access and travel.

How might such a scheme work? For example: a 'basic' or core digital identity might be used for shopping bank utilities, then scale up to a standard identity (basic plus gaming and leisure) and then an enhanced identity (basic, standard and bespoke/overseas). It could be stored in a (digital) 'wallet' and be used with a 'pick and mix' menu with different types of service access.

For such a future scheme to be successful there must be a guarantee that the technology and processes are secure. There must also be a guarantee that the individual has control. Any identity scheme has to be seen as fair with clearly identified responsibilities and accountability.

Future Digital Identity Scheme - Hull's Voluntary and Community Sector

Another possible future scheme is to use an NHS number. British citizens are typically given an NHS number. For those born in Britain this is given at birth. Yet, how many times do we actually use our NHS number? Why is this not used more widely throughout life, as a consistent identity marker from birth? There are shared care models, that already exist and that people may find acceptable as a basis for a digital identity scheme.

Visual Note:

The visual note on the next page shows how all the issues described in this report overlap with each other. The visual note also shows that the following questions were frequently considered when talking about future digital identity schemes:

Who has control?
How do I know it is secure?
How do I know that it is worth the money and the effort?
What can I do if it goes wrong?
Will I become a target for theft by having it?
Will I be forced into a particular form of identity if I have to have one?
Will big brother be watching me?

These questions must be carefully considered and the responses to them co-developed with the public. In order for any future digital identity scheme to be successful it must be recognised that different parts of society will interpret responses to these questions in different ways and indeed will relate to these questions in different ways.

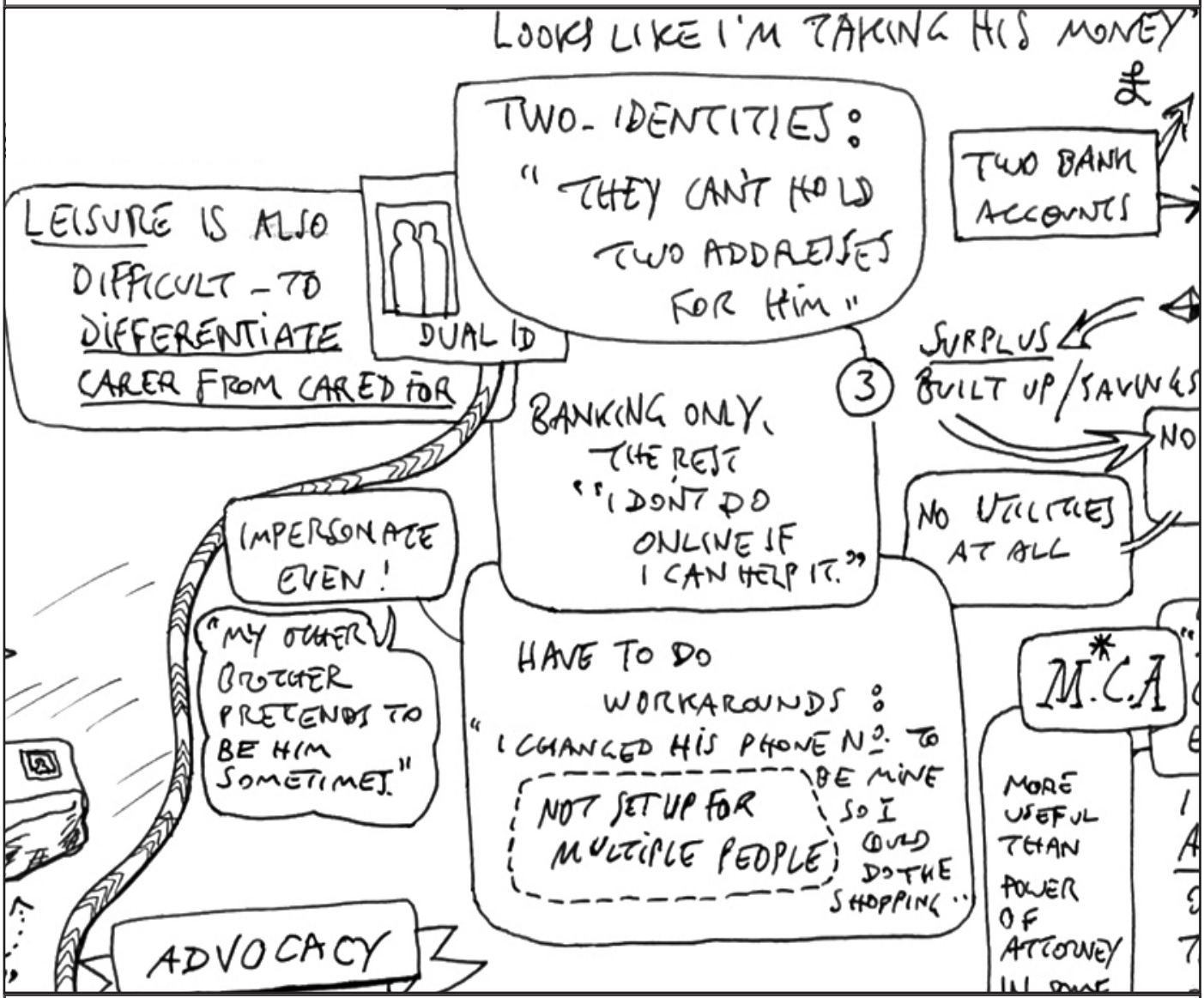
Please see page 7 for the drawing by Claude Heath.


CORE
THE ONE THING THAT DOESN'T CHANGE
MANDATORY
OPTIONAL?
SPECTRUM
CHALLENGES
ONE STOP
HOW TO GET FROM THERE TO HERE?
COMMONALITY
PRISON
NHS NUMBER
GDPR
NORTHBANK FORUM
PRIMARY CARE
VIOLATION OF ME
SHARED DEVICES
LOCKED OUT
WHO HAS CONTROL OF THE ID?
HAS TO BE LEGITIMATE
LITERACY
NOT CLEAR
TWISTED
DATA

DIGITAL IDENTITY

GROUND-UP PERSPECTIVES

Sibs



Royal Holloway University of London
Short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of Digital Identity.
Lizzie Coles-Kemp Information Security Group
Claude Heath Department of Media Arts

September 2020

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Introduction - Sibs

A team at Royal Holloway University of London was commissioned to run a short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of digital identity. DCMS commissioned a programme of 4 consultations to be undertaken with groups who are dependent on digital identities for use of essential, core services such as finance, welfare, health, housing and education. The purpose of the consultation was to provide input on the design of future digital identity schemes; in particular, who should run them and how to make them safe, inclusive and accessible. These consultations are part of a wider call by DCMS for evidence on the topic of digital identity.

Each consultation session was split into two parts: (1). Everyday experiences of digital identity and the challenges faced when managing digital identity, and (2). Requirements for future digital identity schemes.

Due to COVID restrictions, the consultation sessions were held via Zoom. In order to retain the details about the complexity digital identity set-up and use in everyday life, Claude Heath visually illustrated the session using visual note-taking.

This is a report of the consultation session with representatives from the charity **Sibs** that supports those who grow up with or have grown up with a disabled brother or sister. The views expressed are those of this participant group.

Participants:

The 9 participants were all members of the charity Sibs; this is a charity for those with brothers and sisters who are disabled. Sibs members act as advocates for their brothers and sisters (and potentially for other members of their family). This advocacy has many roles but in the digital realm largely revolves around advocating for and carrying out a number of core services on behalf of their sibling. Core services are primarily: financial services (particularly digital banking), health services (particularly managing PIPs, arranging hospital and GP appointments and acting as the intermediary between healthcare professionals and sibling), welfare (particularly welfare claiming and ensuring continuity of payments), day to day care (particularly managing carer's teams and ensuring there is resource in place to cover carer payments and everyday expenses), housing and shopping.

The participants felt largely unseen and unheard as carers and that their role in caring for their sibling is not formally recognised. From their experience, core services recognise parents, recognise partners and recognise children of those who are disabled but not siblings and the ramifications of being unrecognised become more profound as core services become increasingly digital. This is because the siblings' invisibility to formal bureaucratic systems is mirrored in the digital design. It is also important to recognise that standards of proof and the roles of advocates are regulated differently across the devolved nations in the UK.

Everyday Experiences of Digital Identity - Sibs

A key area where digital identity plays an important role in digital advocacy is digital banking. 2-factor authentication is particularly stressful because it assumes that 2-factor authentication will be for one bank account not several (at the same bank) and this makes banking for yourself and your sibling very difficult (and at times impossible). Biometric authentication can be anxiety inducing for the sibling that is being advocated for because it can be a complex process that is difficult to both explain and carry out.

Digital services can also make other aspects of advocacy easier and timesaving (for example on-line shopping) but can make aspects of advocacy more difficult (particularly when it comes to verifying who you are and whether your sibling needs an advocate and why).

Digital services are designed to make tasks more efficient. One of the ways that efficiency is achieved is by making connections between different data and these connections can be misinterpreted. For example, if the bank accounts of two siblings are connected (at the same bank), there can be assumptions that the welfare payments of one sibling is a form of "joint" income – making it difficult for the advocate to apply for loans or welfare in their own right.

NHS access is another area where an instance of an app linked to a phone number cannot be used for two people. The one phone number is a part of the digital identification. As a result, there are examples where the sibling cannot use the phone to make appointments or get test results both for themselves and for the sibling they care for.

A way round these challenges of using apps is to call the service provider – however, it takes a long time to phone up, queue and then have the conversation. This is a problem because siblings are often time pressurised. Advocacy is, in effect, a job that has to be worked around all of their own jobs and responsibilities – this means that advocates are often time-poor, emotionally exhausted and stressed.

The legal systems underpinning advocacy do not provide sufficient granularity and the notion of "capacity" is a contested concept that is treated differently by the various support and social services. Power of attorney is a principle that underpins much of how the digital identity of an individual can be accessed and used by another person. However, the participants were very clear that power of attorney is not a magic bullet. For example, power of attorney does not match to the different levels of advocacy. Power of attorney is expensive to access and it can be difficult to prove levels of capacity (for the sibling who is advocated for), particularly with someone who has fluctuating levels of capacity or who has never been classed as "capacitated". This is further complicated by the sense that many professionals do not understand the role of siblings in terms of caring for a brother or sister and are sometimes more focused on what individuals are capacitated to do rather than what they are not. Examples were given where participants were left to manage unrecognised or fluctuating gaps in their

siblings' capacity using digital systems that did not recognise the legitimacy of their role as carers. This causes considerable stress and potentially places both parties (sibling in caring role and sibling being cared for) in vulnerable situations.

When siblings act as advocates or carers they are often having to transition from an informal form of advocacy (formerly carried out by their parents) to a more formal, visible role – in part as a result of the digital. This causes additional stress. The digital systems have lost the intermediaries who could help with hooking the system into their particular model of care without stress and disruption. Chat Bots and automated calling systems are not able to replicate the benefits of speaking to a real person. The lack of intermediaries pushes the burden of support even more onto the sibling who is undertaking the caring role and the pressure is draining and frustrating – particularly as the pressure is part of a caring role that lasts for many years and is buried into other additional everyday stresses and demands. In addition, the feelings advocates have towards their siblings are complicated and often conflicted; this adds to the stress.

When siblings act as advocates or carers they are often having to prove and re-prove who they are to service providers and government agencies and that their intentions towards their siblings are good and not malicious. Even when you have powers under Power of Attorney or you have proven who you are – you still have to routinely re-prove who you are and why you are advocating on behalf of your sibling. The processes are increasingly adversarial in the sense that service providers seem to have switched to a default position of not believing who you are and assume you are intending harm. The lack of someone to talk to directly means that the complaints process and social media are your only means of resolving problems. This is repetitive and exhausting.

Other examples of where acting as an advocate causes problems with digital identity include: booking travel and booking a holiday. Booking on behalf of someone is difficult and it is often assumed that the advocate is the traveller not the sibling. There is little recourse to fix this.

These difficulties often result in workarounds or trying to second guess/ deconstruct the digital systems. The efficiencies and security controls have trade-offs and hurdles that are proving increasingly difficult to manage. Digital access seems to have to be agreed by committee – and whilst the responsibility sits with the advocate, the authority does not sit with the advocate but with a form of committee. This committee is often composed of other family members as well as external institutions and this is complex as families are often composed of complex and sometimes conflicted relationships.

One of the questions that a future digital identity scheme will need to consider is: how much control over a digital service is enough? Another question that is frequently asked is: How do you have control over your sibling's finances but still respect a sibling's autonomy?

Future Digital Identity Scheme - Sibs

Designing a future identity system with the following benefits would be desirable:

A unified common standard for proving who you are.
Common standards for proof both of identity and of advocacy.
Proving who you are once and to not have to repeat that process.

In addition, the following suggestions were made:

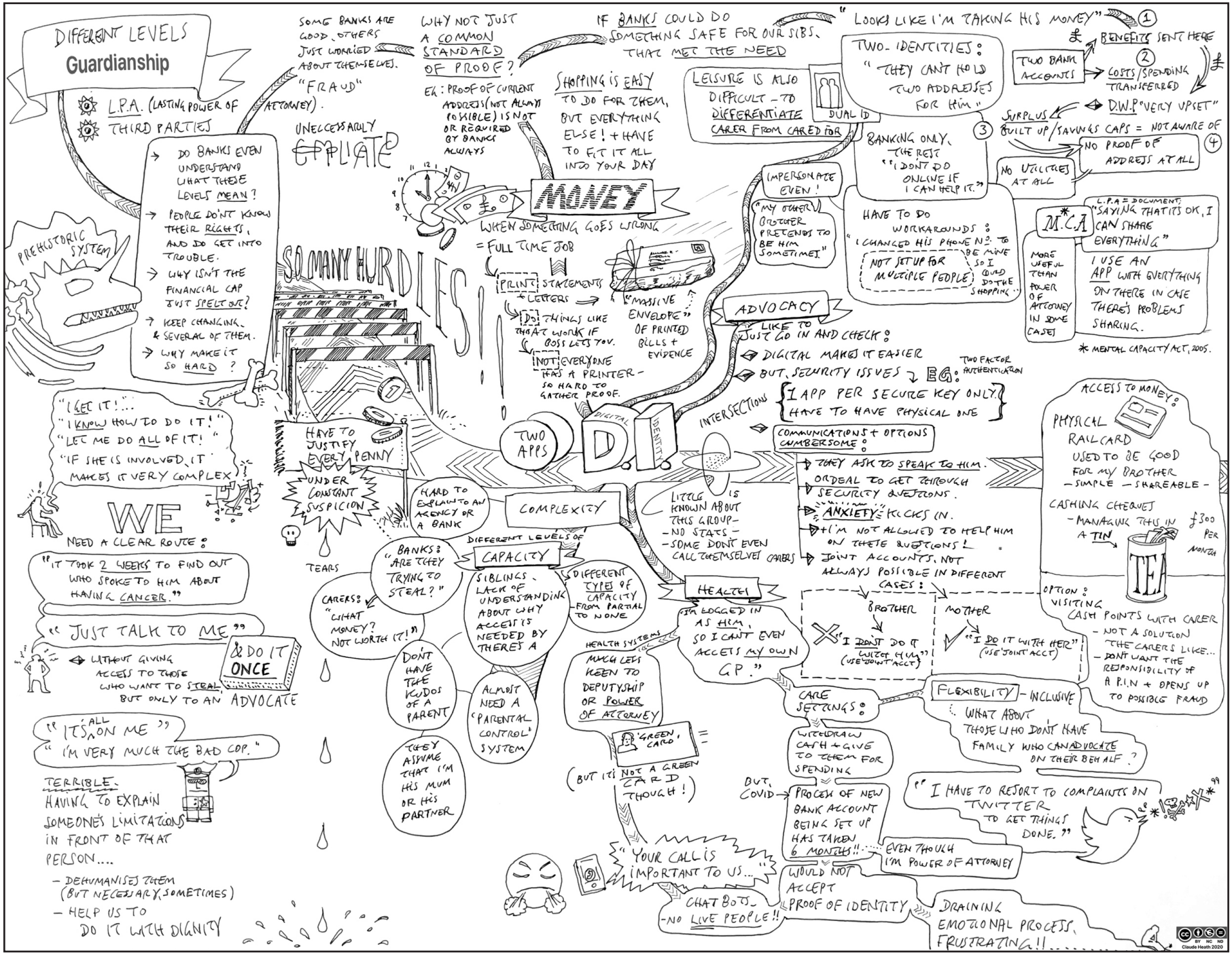
1. Proving that you are legitimately acting on behalf of your sibling should ideally be subject to standardised tests.
2. The work of siblings should be valued and treated with respect and dignity - not with suspicion. Technologies or intermediary supported technologies should be better at differentiating between malicious and benign motivations.
3. Identity systems need to be able to differentiate between the granular levels of guardianship and differing levels of capacity with sufficient flexibility to respond to changes in situation and the subtleties of the notions of both guardianship and capacity.
4. Digital identity systems and services need to be capable of understanding that people can legitimately be the holders of 2+ identities. Authentication for those identity systems also need to be able to authenticate two identities tied to one physical entity (e.g. phone).
5. Identity systems and services also need to be adaptable and supportive – again in recognition of the important labour that advocates do.
6. Not only do the technologies have to be accessible and usable but so too do the laws, regulations and policy systems that these technologies interface with.

Visual Note:

Please see page 6 for the full drawing by Claude Heath.


" JUST TALK TO ME "
& DO IT ONCE
WITHOUT GIVING ACCESS TO THOSE WHO WANT TO STEAL, BUT ONLY TO AN ADVOCATE
" IT'S ALL ON ME "
" I'M VERY MUCH THE BAD COP. "
TERRIBLE.
HAVING TO EXPLAIN SOMEONE'S LIMITATIONS IN FRONT OF THAT PERSON....

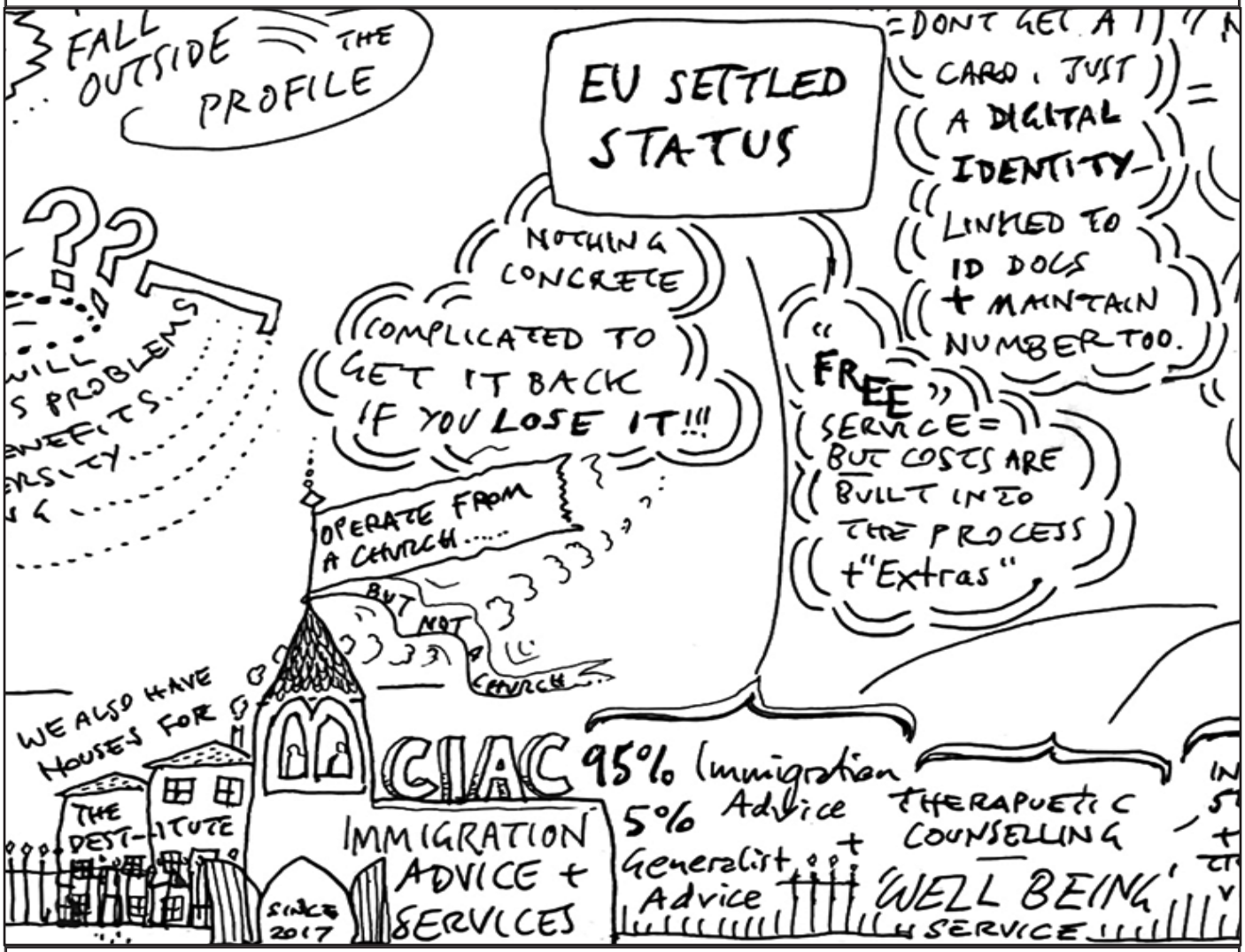

PROCESS OF NEW BANK ACCOUNT BEING SET UP HAS TAKEN 6 MONTHS!!
" I HAVE TO RESORT TO COMPLAINTS ON TWITTER TO GET THINGS DONE. "
EVEN THOUGH I'M POWER OF ATTORNEY
WOULD NOT ACCEPT PROOF OF IDENTITY
DRAINING EMOTIONAL PROCESS, FRUSTRATING!!


DIFFERENT LEVELS
Guardianship
L.P.A. (LASTING POWER OF ATTORNEY).
THIRD PARTIES
SOME BANKS ARE GOOD, OTHERS JUST WORRIED ABOUT THEMSELVES.
"FRAUD"
UNECCESSARILY COMPLICATE
WHY NOT JUST A COMMON STANDARD OF PROOF?
EG: PROOF OF CURRENT ADDRESS (NOT ALWAYS POSSIBLE) IS NOT OR REQUIRED BY BANKS ALWAYS
IF BANKS COULD DO SOMETHING SAFE FOR OUR SIBS, THAT MET THE NEED
SHOPPING IS EASY TO DO FOR THEM, BUT EVERYTHING ELSE! + HAVE TO FIT IT ALL INTO YOUR DAY
"LOOKS LIKE I'M TAKING HIS MONEY"
LEISURE IS ALSO DIFFICULT - TO DIFFERENTIATE CARER FROM CARED FOR
DUAL ID
TWO IDENTITIES: "THEY CAN'T HOLD TWO ADDRESSES FOR HIM"
TWO BANK ACCOUNTS
BENEFITS SENT HERE
COSTS/SPENDING TRANSFERRED
D.W.P "VERY UPSET"
SURPLUS BUILT UP/SAVINGS CAPS = NOT AWARE OF
NO PROOF OF ADDRESS AT ALL
NO UTILITIES AT ALL
BANKING ONLY. THE REST "I DON'T DO ONLINE IF I CAN HELP IT."
IMPERSONATE EVEN!
"MY OTHER HALF/OTHER PRETENDS TO BE HIM SOMETIMES"
HAVE TO DO WORKAROUNDS: "I CHANGED HIS PHONE NO. TO BE MINE SO I COULD DO THE SHOPPING."
NOT SETUP FOR MULTIPLE PEOPLE
M.C.A*
L.P.A = DOCUMENT: "SAYING THAT IT'S OK, I CAN SHARE EVERYTHING"
MORE USEFUL THAN POWER OF ATTORNEY IN SOME CASES
I USE AN APP WITH EVERYTHING ON THERE IN CASE THERE'S PROBLEMS SHARING.
* MENTAL CAPACITY ACT, 2005.
PREHISTORIC SYSTEM
DO BANKS EVEN UNDERSTAND WHAT THESE LEVELS MEAN?
PEOPLE DON'T KNOW THEIR RIGHTS, AND DO GET INTO TROUBLE.
WHY ISN'T THE FINANCIAL CAP JUST SPELT OUT?
KEEP CHANGING & SEVERAL OF THEM.
WHY MAKE IT SO HARD?
MONEY
WHEN SOMETHING GOES WRONG = FULL TIME JOB
SO MANY HURDLES!!
PRINT STATEMENTS + LETTERS
DO THINGS LIKE THAT WORK IF BOSS LETS YOU.
NOT EVERYONE HAS A PRINTER - SO HARD TO GATHER PROOF.
"MASSIVE ENVELOPE" OF PRINTED BILLS + EVIDENCE
ADVOCACY
LIKE TO JUST GO IN AND CHECK:
DIGITAL MAKES IT EASIER
BUT, SECURITY ISSUES ↘ EG: TWO FACTOR AUTHENTICATION
INTERSECTION
1 APP PER SECURE KEY ONLY
HAVE TO HAVE PHYSICAL ONE
COMMUNICATIONS + OPTIONS CUMBERSOME:
"I GET IT!..."
"I KNOW HOW TO DO IT!"
"LET ME DO ALL OF IT!"
"IF SHE IS INVOLVED, IT MAKES IT VERY COMPLEX!"
HAVE TO JUSTIFY EVERY PENNY
UNDER CONSTANT SUSPICION
TWO APPS
D.I.
DIGITAL IDENTITY
WE
NEED A CLEAR ROUTE:
"IT TOOK 2 WEEKS TO FIND OUT WHO SPOKE TO HIM ABOUT HAVING CANCER."
"JUST TALK TO ME"
& DO IT ONCE
WITHOUT GIVING ACCESS TO THOSE WHO WANT TO STEAL, BUT ONLY TO AN ADVOCATE
"IT'S ALL ON ME"
"I'M VERY MUCH THE BAD COP."
TERRIBLE.
HAVING TO EXPLAIN SOMEONE'S LIMITATIONS IN FRONT OF THAT PERSON....
- DEHUMANISES THEM (BUT NECESSARY, SOMETIMES)
- HELPS US TO DO IT WITH DIGNITY
HARD TO EXPLAIN TO AN AGENCY OR A BANK
TEARS
COMPLEXITY
DIFFERENT LEVELS OF CAPACITY
BANKS: "ARE THEY TRYING TO STEAL?"
CARERS: "WHAT MONEY? NOT WORTH IT!"
SIBLINGS - LACK OF UNDERSTANDING ABOUT WHY ACCESS IS NEEDED BY THERE'S A
DIFFERENT TYPES OF CAPACITY FROM PARTIAL TO NONE
DON'T HAVE THE KUDOS OF A PARENT
ALMOST NEED A 'PARENTAL CONTROL' SYSTEM
THEY ASSUME THAT I'M HIS MUM OR HIS PARTNER
LITTLE IS KNOWN ABOUT THIS GROUP - NO STATS - SOME DON'T EVEN CALL THEMSELVES CARERS
THEY ASK TO SPEAK TO HIM.
ORDEAL TO GET THROUGH SECURITY QUESTIONS.
"ANXIETY" KICKS IN.
+ I'M NOT ALLOWED TO HELP HIM ON THESE QUESTIONS!
JOINT ACCOUNTS, NOT ALWAYS POSSIBLE IN DIFFERENT CASES:
BROTHER
MOTHER
"I DON'T DO IT WITH HIM" (USE 'JOINT ACCT')
"I DO IT WITH HER" (USE 'JOINT ACCT')
HEALTH
I'M LOGGED IN AS HIM, SO I CAN'T EVEN ACCESS MY OWN GP."
HEALTH SYSTEMS MUCH LESS KEEN TO DEPUTYSHIP OR POWER OF ATTORNEY
'GREEN CARD' = (BUT IT'S NOT A GREEN CARD THOUGH!)
"YOUR CALL IS IMPORTANT TO US..."
CHAT BOTS - NO LIVE PEOPLE!!
ACCESS TO MONEY:
PHYSICAL
RAILCARD
USED TO BE GOOD FOR MY BROTHER
- SIMPLE - SHAREABLE -
CASHING CHEQUES
- MANAGING THIS IN A TIN
£300 PER MONTH
TIN
OPTION: VISITING CASH POINTS WITH CARER
- NOT A SOLUTION
THE CARERS LIKE...
- DON'T WANT THE RESPONSIBILITY OF A P.I.N + OPENS UP TO POSSIBLE FRAUD
CARE SETTINGS:
FLEXIBILITY - INCLUSIVE
WHAT ABOUT THOSE WHO DON'T HAVE FAMILY WHO CAN ADVOCATE ON THEIR BEHALF?
WITHDRAW CASH + GIVE TO THEM FOR SPENDING
BUT, COVID → PROCESS OF NEW BANK ACCOUNT BEING SET UP HAS TAKEN 6 MONTHS!!
EVEN THOUGH I'M POWER OF ATTORNEY
WOULD NOT ACCEPT PROOF OF IDENTITY
"I HAVE TO RESORT TO COMPLAINTS ON TWITTER TO GET THINGS DONE."
DRAINING EMOTIONAL PROCESS. FRUSTRATING!!
BY NC ND
Claude Heath 2020

DIGITAL IDENTITY

GROUND-UP PERSPECTIVES

Community Integration and Advocacy Centre (CIAC)



Royal Holloway University of London
Short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of Digital Identity.
Lizzie Coles-Kemp Information Security Group
Claude Heath Department of Media Arts

September 2020

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Introduction - CIAC

A team at Royal Holloway University of London was commissioned to run a short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of digital identity. DCMS commissioned a programme of 4 consultations to be undertaken with groups who are dependent on digital identities for use of essential services such as finance, welfare, health, housing and education. The purpose of the consultation was to provide input on the design of future digital identity schemes; in particular, who should run them and how to make them safe, inclusive and accessible. These consultations are part of a wider call for evidence on the topic of digital identity.

Each consultation session was split into two parts: (1). Everyday experiences of digital identity and the challenges faced when managing digital identit, amd (2). Requirements for future digital identity schemes.

Due to COVID restrictions, the consultation sessions were held via Zoom. In order to retain the details about the complexity digital identity set-up and use in everyday life, Claude Heath, visually illustrated the session using visual note-taking.

This is a report of the consultation session with representatives from **CIAC**, an organisation which is OISC regulated to provide immigration advice and support. The views expressed are those of this participant group.

Participants - Community Integration and Advocacy Centre (CIAC):

Four representatives from CIAC took part in this session. The representatives include CIAC's Chief Executive Officer and 3 volunteers. CIAC was founded in 2017 and is a registered charity that supports emerging communities to contribute fully to life in the UK as committed and active citizens. Emerging communities include refugees, asylum seekers, refused asylum seekers, EEA migrants and other migrants. CIAC also provides services to those who are victims of modern slavery and human trafficking. 95% of the services that CIAC provides are immigration services with 5% as generalist services covering welfare issues, accommodation advice, debt advice and asylum support, and helping people where there are difficulties in evidencing long term residence in the UK. Those with an income are asked to pay for the support received, with 25% of each payment going to a destitution fund - covering the costs of providing services to those who are destitute. There is also an intention to expand CIAC services to provide therapeutic emotional and well-being services for those suffering from trauma induced by forced immigration, slavery, trafficking and other life situations exacerbated by resettlement.

As a guiding principle, CIAC provides services that enable people to become self-sufficient through realising the rights that their identity affords them. The belief underpinning this principle is that if people can realise the rights that they are entitled to, they can realise a safe and secure future. This session therefore highlighted the fact

that an identity has rights attached to it and any digital identity scheme has to respect and support those rights. The participants were very aware of the difficulties faced by those not attaining citizenship and once those rights are realised access to basic and core services becomes more realisable and less precarious.

Volunteers have many reasons for joining CIAC: some have an education related to immigration services, some have first or second-hand experience of migration and of the challenges of re-settling in a new land, and some have been recipients of support from CIAC. The participants reflect great diversity, incorporating people of Irish, Hungarian, Moroccan and Spanish nationalities.

Volunteering at CIAC is a complex and detailed process. Volunteers develops skills and experience related to both the very detailed, technical knowledge required to provide immigration services and also the human interaction skills and practices of care needed to successfully deliver such services. The process for learning these skills and acquiring these experiences is to shadow a more experienced volunteer or member of staff. Volunteers can also obtain formal qualifications through Office of the Immigration Services Commissioner. The success of CIAC is evidenced through the word of mouth recommendations and the volume of requests for their services.

Everyday Experiences of Digital Identity:

It emerged during the session that not only do volunteers need to acquire detailed immigration knowledge and the skills to work with people, volunteers also need to develop a good understanding of IT and how digital immigration services work, as well as the acute problems that immigrants can face when accessing digital services. These problems include: lack of money to access technology or the internet, limited English, limited formal education, low levels of IT skills and low levels of literacy. These problems conspire to create problems when applying for services that require a digital identity.

The clearest example of digital identity in action in the immigration services context is the process to apply for EU settled status. The process is entirely digital and requires that you (a). have access to the EU settled status app (b). have access to the internet (c). have access to an email address (d). have access to evidence that can prove that you have the right to remain in the UK under this scheme. This is a difficult process if the applicant does not have the following resources:

(1) Technical and data access
(2) A stable email address
(3) Confident English language skills
(4) Clear evidence of British residence.

Everyday Experiences of Digital Identity - CIAC

Common problems for applicants relate to losing access to the email address to which the application is attached. This is a common problem if the email address is incorrectly entered, or the email address is temporary. Once the email address is lost, the application is extremely difficult to recover. Another problem is not completing the application and interrupting part-way through. It is difficult to suspend an application and then recommence it. A further problem is not having access to the relevant information to prove residency, including not having access to the passport that proves nationality and citizenship in the old land. The process can also become stressful if applicants have limited or no access to the internet, have to borrow a phone to make the application but then have to access their email through their own phone to confirm the application.

The EU settled status scheme is a good example of a digital-only scheme - issuing a purely digital identity. The participants noted that many of those applying for CIAC's services prefer a physical card to prove their identity, rather than relying on an exclusively digital proof of identity, as the digital version is most likely to be stored on devices that may be too expensive and, if such a device is owned, is difficult to replace if lost. There is also a sense of security and safety that comes from a physical representation of an approved identity that many do not have with a digital proof of identity.

Digital identity schemes are typically designed on the assumption that a person's name is uncontested. The immigration journey often results in changes to a person's name and yet there is no consistent way, even internally within a government, as to how departments will treat name changes and this can cause problems when a person tries to prove who they are. This makes it very difficult for volunteers and the people they are supporting to know how to handle name changes within an identity application or verification process.

The more that the immigration services become digital, the harder and more expensive it becomes to resolve proof and verification issues. This is partly because the policy on immigration has become more hostile, and partly because the IT that supports digital services is either not fit for purpose, or is not usable for various immigrant groups. The important point to note is that a hostile policy and poorly designed IT have security impacts (as outlined in the following examples) that not only make an immigrant more vulnerable to fraud but also damage the relationship between the individual, their kin and friendship network and the state. These security outcomes have potentially adverse ramifications for the individuals and also for a state that is increasingly reliant on compliant digital use as a means of governing its peoples.

A significant barrier to immigrants successfully obtaining a digital identity is a lack of support when the digital identity application process goes wrong. Whilst telephone resolution services are sometimes offered, the calls are expensive and the response rate is low. If the resolution service is on-line, the service is often confusing

and resolution is not guaranteed. The more digital that these services become, and the harder it is to access those resolution services, then immigrants turn to “friends” who attempt to complete the services on their behalf. Sometimes this is successful, sometimes not. However, it does mean that the person can lose control of their application, making it difficult at times to resolve issues related to an application. It also increases the likelihood of identity fraud because valuable information that proves who a person is, is handed over to another person. The view was put forward that identity fraud is more likely to come from within the community. It was also viewed as a strong possibility that digital identity schemes will increase the likelihood of identity fraud if the digital identity schemes are difficult to access, and have costs attached to them, because people will be forced to rely on informal help - and this makes them vulnerable.

One particular area of potential digital identity fraud is the scenario where those who are trafficking people from the EU, use the EU settled status scheme to apply in the name of those who are being trafficked and/or enslaved, either through manipulation or through the threat of violence. Once the digital identities come through, they can be used for nefarious activities by those running the slavery and trafficking schemes.

The participants noted that as the immigration environment has become more hostile, the digital immigration services and the associated identity verification services have also become more hostile. It has become harder to navigate these processes, and less support is available via digital means. There is a very strong sense that digital services are being used to police the borders from within the country, and that an applicant has to prove that they have rights, and that they are not trying to defraud the system. Increasingly this proof comes via digital means (e.g. biometrics) and yet the digital means of proof cost money, money that applicants often do not have. Even for free immigration services, the digital proof is charged for, and the charging is enforced by digital means. The logistics and administration related to arranging digital proof is also expensive (which for example includes travel). This is not designed to support or accommodate the particular precarities that immigrants and their families often face (money, time, language, technical ability for instance). The CIAC volunteers often find themselves trying to reduce the adverse impacts on immigrants of poorly designed technology, complex processes and conflicting rules.

There is a concern that digital identity will mean greater surveillance. One example was given in relation to the ASPEN card - a digital payment card that relates to asylum seekers in receipt of asylum support under Sections 95/4 of the Asylum Act.. This was reported to be used to track where immigrants, who are in receipt of ASPEN payments, travel to, spend their money, and can be used to identify what they spend their money. It is important to note that regardless of whether surveillance is intended or not, in the context of a digital identity scheme, the experiences related to the ASPEN card will mean that it is likely that surveillance will be assumed by some groups of

immigrants. This means that a digital identity will have a different symbolic power for different groups. A comparison with the Spanish identity scheme was given: the Spanish system is partially digital and it was suggested that the way that the system is perceived, depends on how vulnerable a group feels within society, and upon the type of relationship that the group has with the state.

The ASPEN card experience described above also reveals how immigrants from some backgrounds have very little experience with technologies, and are not familiar with how technology-enabled banking works. Volunteers therefore on occasion also have to help immigrants set-up bank accounts. The sense is often that banks are trying to find reasons to not accept immigrants as customers - the standards of evidence required to obtain a banking identity is often complex, difficult to understand, hard to obtain, and is not standardised.

Future Digital Identity Scheme - Aspirations, Hopes and Fears:

The participants counselled that the introduction of a digital identity scheme had to be very carefully managed within immigration communities. The introduction of such a scheme has to be attentive to the precarities and vulnerabilities that immigrants can experience and the poor experiences that many of them have had with digital immigration systems in the UK and elsewhere for such a scheme to be successful. The precarities and vulnerabilities together with the poor experiences related here, mean that trust and confidence in a new digital identity system will be low - this will make compliance and use of the system less predictable. As a result, it is essential that such a service is supported by people that immigrants can talk to and that can support their use of a digital identity service.

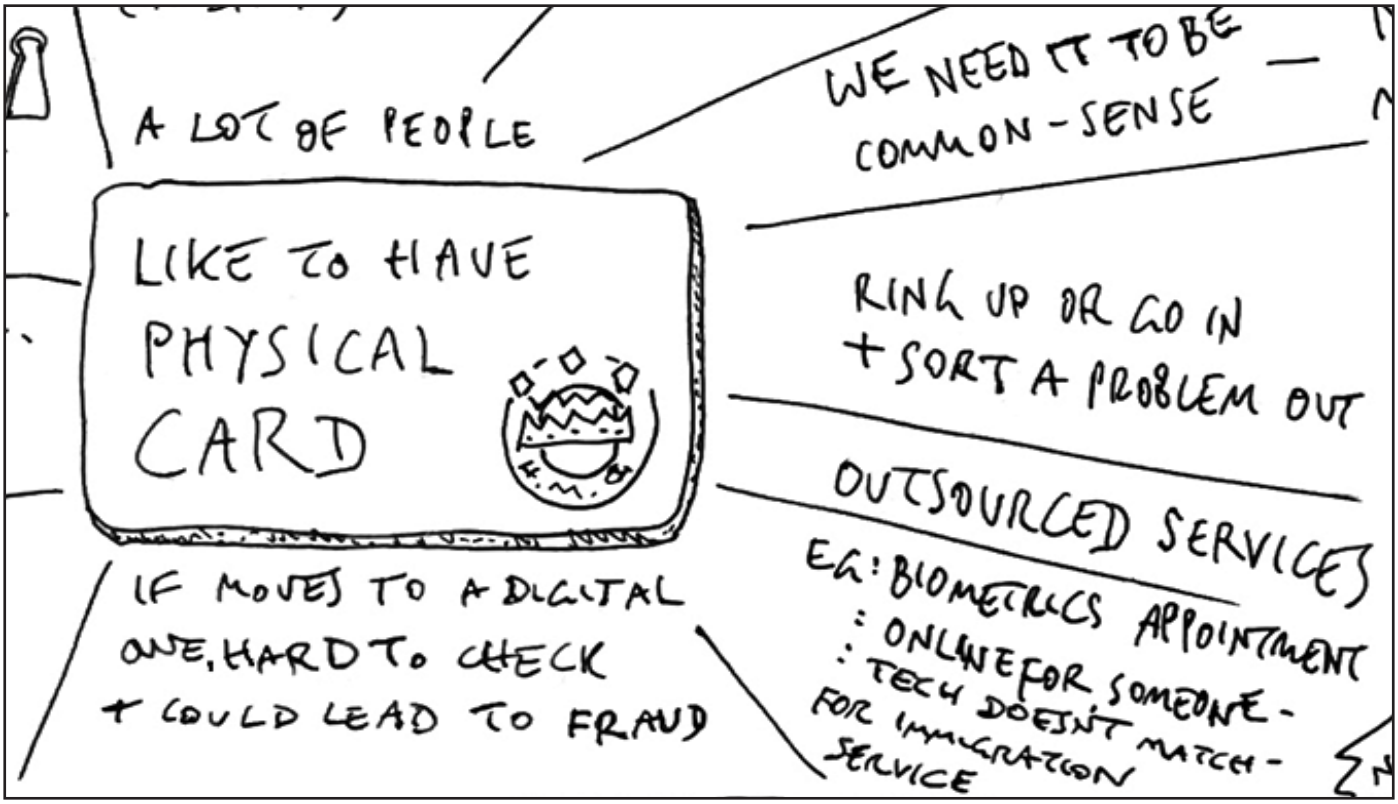
A digital identity scheme applied to immigrants needs to be designed with the risks to immigrants in mind and a recognition that errors in applications for immigration status can be catastrophic for the applicant, with no option for redress or for claiming back the considerable sums of money that are sometimes spent.

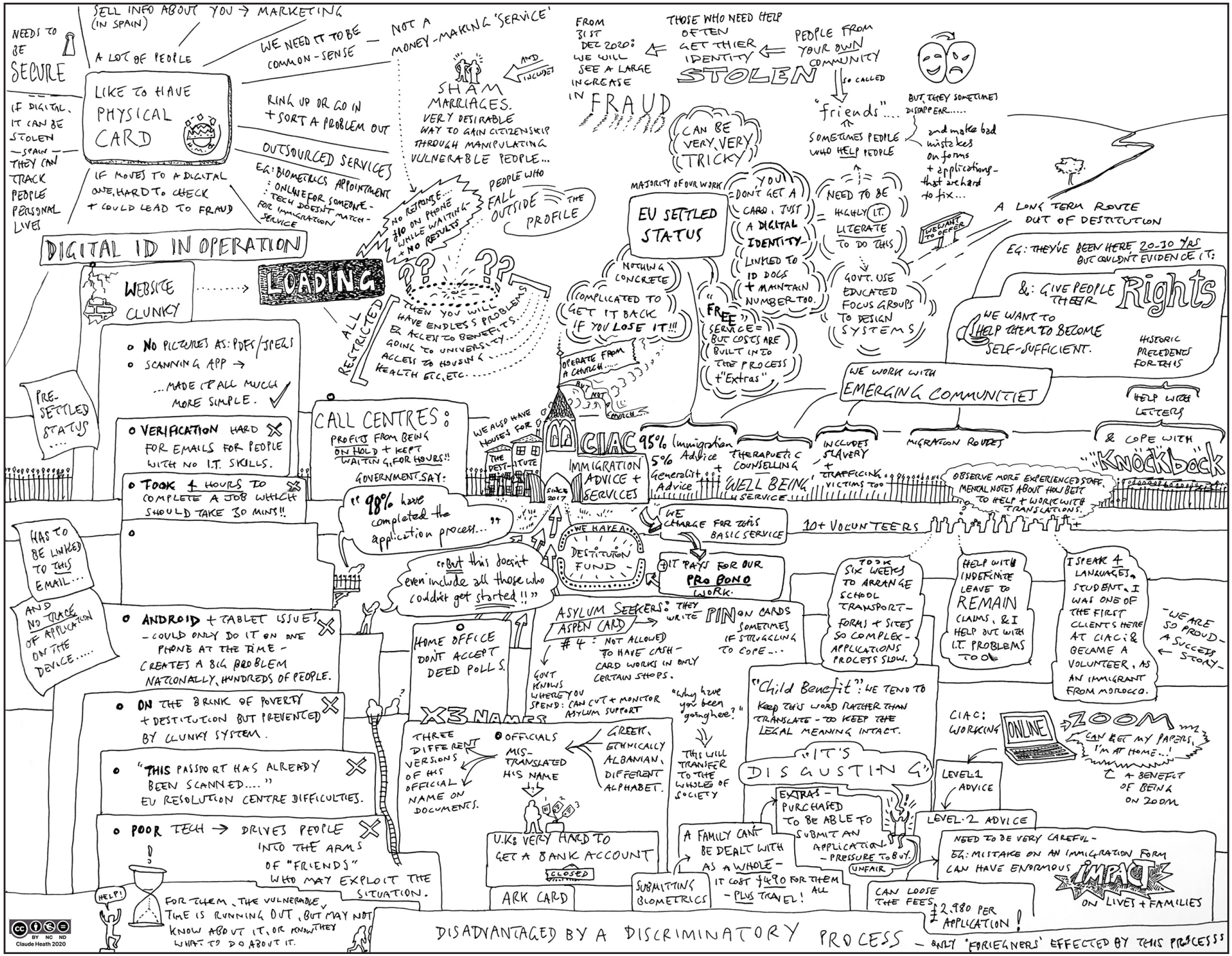
A digital identity scheme needs to have a fair and transparent funding model attached to it, so that it is not perceived as a scheme that discriminates against particular groups, or that amplifies existing discriminations. A digital identity scheme must also be secure and the use of personal data needs to be ethical for the system to be trusted. The participants queried how possible it is to have a fair and transparent funding model, and with this, ethical use of data, when digital systems are often outsourced to many parties outside government. The current experience with existing digital immigration systems was that no one is seen to be responsible for ensuring that immigrants have fair and equitable access to the digital systems, and that a digital identity is not designed with the value to the immigrant in mind.

Future Digital Identity Scheme - CIAC

From CIAC's point of view, the realisation of one's rights in a country is a means of empowerment - and enables the securing of a future in that country that has value both to the individual and to the land to which they have come. Such forms of empowerment provide autonomy and control for the individual, and thus any future digital identity scheme must also support and engender autonomy and control.

Visual Note:

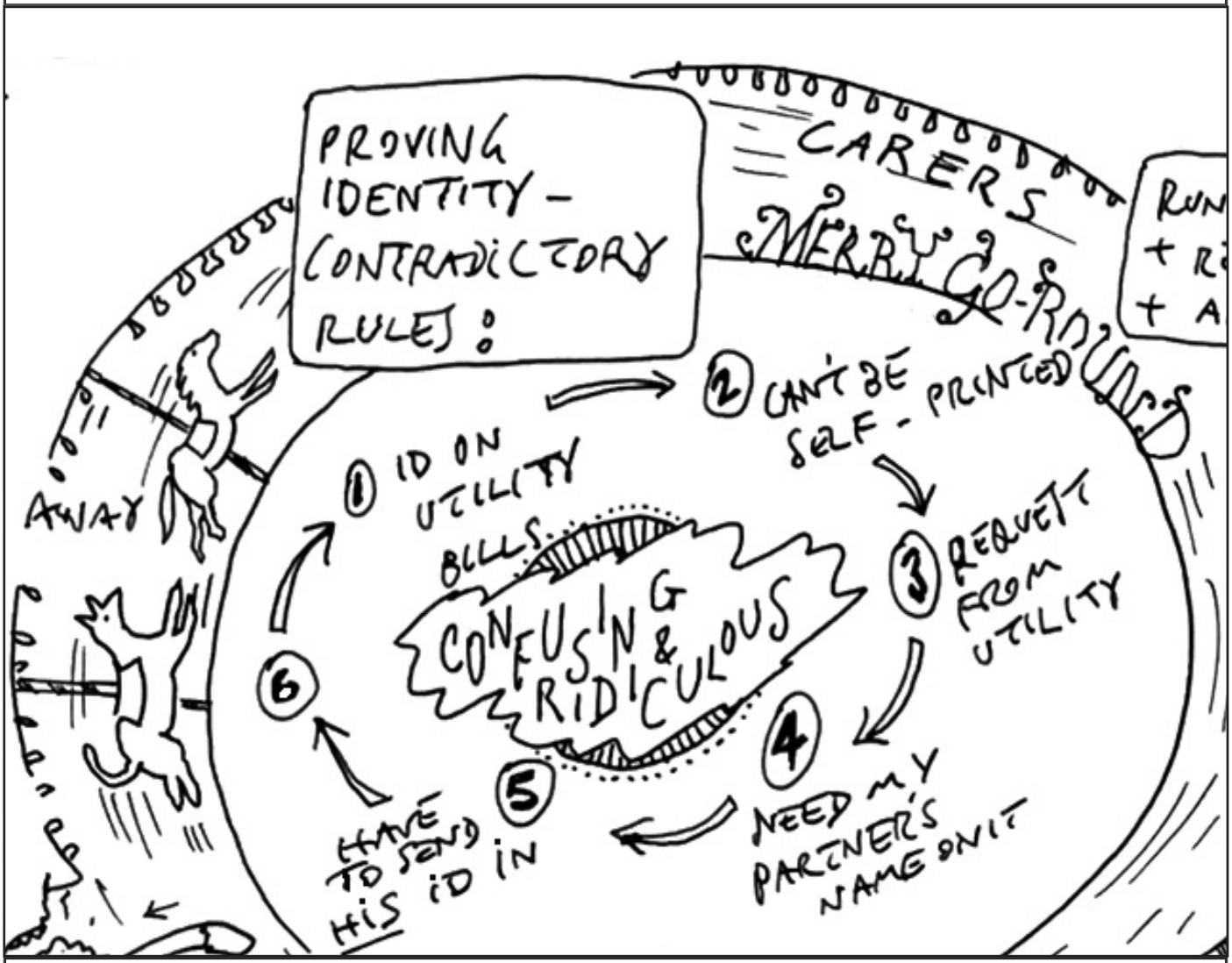



NEEDS TO BE SECURE
SELL INFO ABOUT YOU → MARKETING (IN SPAIN)
A LOT OF PEOPLE
WE NEED IT TO BE COMMON-SENSE
NOT A MONEY-MAKING 'SERVICE'
LIKE TO HAVE PHYSICAL CARD
IF DIGITAL, IT CAN BE STOLEN — SPAIN — THEY CAN TRACK PEOPLE PERSONAL LIVES
RING UP OR GO IN + SORT A PROBLEM OUT
OUTSOURCED SERVICES
EG: BIOMETRICS APPOINTMENT: ONLINE FOR SOMEONE - TECH DOESN'T MATCH - FOR IMMIGRATION SERVICE
IF MOVES TO A DIGITAL ONE, HARD TO CHECK + COULD LEAD TO FRAUD
SHAM MARRIAGES.
VERY DESIRABLE WAY TO GAIN CITIZENSHIP THROUGH MANIPULATING VULNERABLE PEOPLE...
AND INCLUDES
FROM 31ST DEC 2020: WE WILL SEE A LARGE INCREASE IN FRAUD
THOSE WHO NEED HELP OFTEN GET THIER IDENTITY STOLEN
PEOPLE FROM YOUR OWN COMMUNITY
SO CALLED "friends"....
SOMETIMES PEOPLE WHO HELP PEOPLE
BUT THEY SOMETIMES DISAPPEAR.....
AND MAKE BAD MISTAKES ON FORMS + APPLICATIONS - THAT ARE HARD TO FIX...
CAN BE VERY, VERY TRICKY
PEOPLE WHO FALL OUTSIDE THE PROFILE
DIGITAL ID IN OPERATION
LOADING
NO RESPONSE... ON PHONE WHILE WAITING + NO RESULTS
ALL RESTRICTED
THEN YOU WILL HAVE ENDLESS PROBLEMS ER ACCESS TO BENEFITS... GOING TO UNIVERSITY... ACCESS TO HOUSING + HEALTH ETC, ETC.
WEBSITE CLUNKY
NO PICTURES AS: PDFS/JPEGS
SCANNING APP → ...MADE IT ALL MUCH MORE SIMPLE.
PRE-SETTLED STATUS....
VERIFICATION HARD FOR EMAILS FOR PEOPLE WITH NO I.T. SKILLS.
TOOK 4 HOURS TO COMPLETE A JOB WHICH SHOULD TAKE 30 MINS!!
HAS TO BE LINKED TO THIS EMAIL...
AND NO TRACE OF APPLICATION ON THE DEVICE.....
ANDROID + TABLET ISSUES - COULD ONLY DO IT ON ONE PHONE AT THE TIME - CREATES A BIG PROBLEM NATIONALLY, HUNDREDS OF PEOPLE.
ON THE BRINK OF POVERTY + DESTITUTION BUT PREVENTED BY CLUNKY SYSTEM.
"THIS PASSPORT HAS ALREADY BEEN SCANNED...." EU RESOLUTION CENTRE DIFFICULTIES.
POOR TECH → DRIVES PEOPLE INTO THE ARMS OF "FRIENDS" WHO MAY EXPLOIT THE SITUATION.
HELP!
FOR THEM, THE VULNERABLE, TIME IS RUNNING OUT, BUT MAY NOT KNOW ABOUT IT, OR KNOW THEY WHAT TO DO ABOUT IT.
EU SETTLED STATUS
MAJORITY OF OUR WORK
YOU DON'T GET A CARD, JUST A DIGITAL IDENTITY - LINKED TO ID DOCS + MAINTAIN NUMBER TOO.
NOTHING CONCRETE
COMPLICATED TO GET IT BACK IF YOU LOSE IT!!!
"FREE" SERVICE = BUT COSTS ARE BUILT INTO THE PROCESS + "Extras"
NEED TO BE HIGHLY I.T. LITERATE TO DO THIS
GOVT. USE EDUCATED FOCUS GROUPS TO DESIGN SYSTEMS
RELUCTANT TO OFFER
A LONG TERM ROUTE OUT OF DESTITUTION
EG: THEY'VE BEEN HERE 20-30 YRS BUT COULDN'T EVIDENCE IT:
&: GIVE PEOPLE THEIR Rights
WE WANT TO HELP THEM TO BECOME SELF-SUFFICIENT.
HISTORIC PRECEDENTS FOR THIS
WE WORK WITH EMERGING COMMUNITIES
HELP WITH LETTERS
& COPE WITH "KNOCKBACK"
CALL CENTRES: PROFITS FROM BEING ON HOLD + KEPT WAITING FOR HOURS!!
GOVERNMENT SAY: "98% have completed the application process..."
"But this doesn't even include all those who couldn't get started!!"
OPERATE FROM A CHURCH.....
BUT NOT A CHURCH
WE ALSO HAVE HOUSES FOR
THE DESTITUTE
CIAC
IMMIGRATION ADVICE + SERVICES
95% Immigration Advice + 5% Generalist Advice
THERAPEUTIC COUNSELLING + WELL BEING SERVICE
INCLUDES SLAVERY + TRAFFICKING VICTIMS TOO
MIGRATION ROUTES
OBSERVE MORE EXPERIENCED STAFF, MENTAL NOTES ABOUT HOW BEST TO HELP + WORK WITH TRANSLATIONS.
WE HAVE A DESTITUTION FUND
WE CHARGE FOR THIS BASIC SERVICE
IT PAYS FOR OUR PRO BONO WORK.
10+ VOLUNTEERS
HOME OFFICE DON'T ACCEPT DEED POLLS.
X3 NAMES?
THREE DIFFERENT VERSIONS OF HIS OFFICIAL NAME ON DOCUMENTS.
OFFICIALS MIS-TRANSLATED HIS NAME
GREEK, ETHNICALLY ALBANIAN, DIFFERENT ALPHABET.
ASYLUM SEEKERS: ASPEN CARD #4: NOT ALLOWED TO HAVE CASH - CARD WORKS IN ONLY CERTAIN STORES.
GOVT KNOWS WHERE YOU SPEND: CAN CUT + MONITOR ASYLUM SUPPORT
"Why have you been going here?"
THEY WRITE PIN ON CARDS SOMETIMES IF STRUGGLING TO COPE...
THIS WILL TRANFER TO THE WHOLES OF SOCIETY
U.K: VERY HARD TO GET A BANK ACCOUNT
CLOSED
ARK CARD
SUBMITTING BIOMETRICS
A FAMILY CAN'T BE DEALT WITH AS A WHOLE - IT COST £490 FOR THEM ALL - PLUS TRAVEL!
TOOK SIX WEEKS TO ARRANGE SCHOOL TRANSPORT - FORMS + SITES SO COMPLEX - APPLICATIONS PROCESS SLOW.
HELP WITH INDEFINITE LEAVE TO REMAIN CLAIMS, & I HELP OUT WITH I.T. PROBLEMS TOO
I SPEAK 4 LANGUAGES, STUDENT, I WAS ONE OF THE FIRST CLIENTS HERE AT CIAC; & BECAME A VOLUNTEER, AS AN IMMIGRANT FROM MOROCCO.
"WE ARE SO PROUD - A SUCCESS STORY"
"Child Benefit": WE TEND TO KEEP THIS WORD RATHER THAN TRANSLATE - TO KEEP THE LEGAL MEANING INTACT.
"IT'S DISGUSTING"
EXTRAS - PURCHASED TO BE ABLE TO SUBMIT AN APPLICATION - PRESSURE TO BUY.
UNFAIR
CIAC: WORKING ONLINE
ZOOM
CAN GET MY PAPERS, I'M AT HOME...!
A BENEFIT OF BEING ON ZOOM
LEVEL 1 ADVICE
LEVEL 2 ADVICE
NEED TO BE VERY CAREFUL - EG: MISTAKE ON AN IMMIGRATION FORM CAN HAVE ENORMOUS IMPACT ON LIVES + FAMILIES
CAN LOOSE THE FEES £2,980 PER APPLICATION!
DISADVANTAGED BY A DISCRIMINATORY PROCESS - ONLY 'FOREIGNERS' EFFECTED BY THIS PROCESS
Claude Heath 2020

DIGITAL IDENTITY

GROUND-UP PERSPECTIVES

Intergenerational Women



Royal Holloway University of London
Short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of Digital Identity.
Lizzie Coles-Kemp Information Security Group
Claude Heath Department of Media Arts

September 2020

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Introduction - Intergenerational Women

A team at Royal Holloway University of London was commissioned to run a short consultation programme on behalf of The Department for Digital, Culture, Media and Sport (DCMS) on the topic of digital identity. DCMS commissioned a programme of 4 consultations to be undertaken with groups who are dependent on digital identities for use of essential services such as finance, welfare, health, housing and education. The purpose of the consultation was to provide input on the design of future digital identity schemes; in particular, who should run them and how to make them safe, inclusive and accessible. These consultations are part of a wider call for evidence on the topic of digital identity.

Each consultation session was split into two parts: (1). Everyday experiences of digital identity and the challenges faced when managing digital identity, and (2). Requirements for future digital identity schemes.

Due to COVID restrictions, the consultation sessions were held via Zoom. In order to retain the details about the complexity digital identity set-up and use in everyday life, Claude Heath visually illustrated the session using visual note-taking.

This is a report of the consultation session with an **intergenerational group of women** who rely on digital identity for receipt of essential services in a variety of ways. The views expressed are those of this participant group.

Participants - intergenerational women:

4 participants between age 38 and 68 were recruited for this consultation group. All four met the criteria of being dependent on digital identities, either for themselves or for other people. Two women were self-employed, one woman is retired and former business owner, two women have a second income stream from self-owned businesses. All participants are British passport holders, one passport holder is a dual citizen and one woman lives in France.

Everyday Experiences of Digital Identity:

Examples were given of the need to use digital identities for shopping, banking, accessing health services and leisure activities. Examples were also given of where individuals advocated for or vouched for others who were in pursuit of a digital identity. All participants identified that there are bureaucratic challenges if the right paperwork is missing and/or an identity applicant struggles to follow the process. An example was given of trying to prove identity in order to obtain a replacement bank card. In this example, even if the applicant has the right paperwork, presenting that paperwork can be complicated and idiosyncratic. The group concluded that those applying for a digital identity or using a digital identity for essential core services have to be organised and patient. It also helps if there are friends and family as a support network to give advice

as to what to do or to help with the administrative processes.

It was noted that if someone is experiencing stress or anxiety, it can be extremely stressful and unpleasant to be asked to prove identity when challenged. It can also feel overwhelming to be constantly having to prove identity, and this can sometimes result in people dropping out of the identity process or limiting their options so as to avoid identity bureaucracy. This is particularly the case when the process seems unnecessarily complex or adversarial.

Finding the right source of proof can also be stress-inducing. For example, utility bills are often a proof of address for the person trying to prove their identity but the format that the bill comes in is not always right for the type of proof required. The named individual on the bill may also not identify the person claiming identity. There are also contradictions in the different processes for proving identity: for example, in person you may have to present several specific pieces of evidence to acquire a replacement bank card. But, via a banking app, you might only need to use your PIN to access the app and from there you can order a replacement card.

It was felt that the challenges facing older users sometimes go unacknowledged. Elderly groups can also struggle to verify their identity: these are groups that are less likely to have passports or driver's licence. At the same time, elderly groups are being encouraged to use on-line services for day to day activities. Elderly access to digital services and proving who they are on-line is another example of where community support is needed, because often the elderly require care and support to carry out the digital bureaucratic processes, and support to make sure that they can continue to re-validate their identities.

However, having a validated identity is only part of what is needed. These identities also have to be useful by enabling access to useful information or services. This means that the digital identity must access services that are useful and it is this that makes a digital identity valuable. An example was given of the NHS number – where everyone has a unique NHS number but providing this is not enough to get access to your own health data, change GP surgeries or to have medical data shared between two clinical teams, with an example given of someone with a serious condition who personally has to carry her file from one consultation to the next. This was contrasted with Spain where a Spanish citizen has a unique identity number, this number does not have to be re-validated , gives you access to essential services and is also your Tax ID. Everyone in Spain is able, it was said, to quote their number from memory [it is compulsory to carry ID at all times]. A further example was given of where British citizens in Spain can encounter difficulties when selling a property, for example, as their passport number will have changed upon renewal over time and may no longer match the details on the deed of purchase. A Notary is then required to certify the identity of the British person with different passport numbers. The system in Spain might perhaps suit criminals who do not wish to have their Spanish Foreigner´s ID

(which does not change) linked to their current UK passport number.

The attitudes towards digital identity vary depending on your experiences of identity, and of the safety and security of that identity. Examples were given of how older people might not be of the mindset that is necessary to take active steps to protect a digital identity and how, as a result, older people can easily be conned. This means that older people need to be suspicious of unsolicited offers of help and support but nevertheless still remain able to receive support.

The group discussed the pros and cons of a single identity: not only might a single digital identity be used for essential services but also for browsing, for shopping and for leisure activities (e.g. Netflix). However, whilst this might make life easier, it potentially makes you open to attack and manipulation and where attack and manipulation might be by the service provider itself as well as malicious third parties.

Future Digital Identity Scheme - Aspirations, Hopes and Fears:

In a notional future, the groups discussed the possibility of a basic identity for core, essential services that everyone needs access to. There might be additional services for which someone could use the identity but these would be additional identity services.

The group agreed that such an identity has to be secure, easy to use and be reliable for all people regardless of their competencies. The group argued that there has to be the right kind of support in place for those who need it to be able to make decisions regarding digital identity and for them to be able to use it fully.

Those who run the services have to be accountable and the ownership of these responsibilities has to be transparent. The sentiment was articulated that as a society we are being pushed down the digital access route but as individuals and as a society we need some control over how our identities are being handled. The managers of the identity systems should be accountable and responsible to us. If there is no control and transparency, then a future digital identity result in us being fed whatever an algorithm matches to us and we could lose control over our use of digital services. At present, there is a sense of taking back control when you deliberately wrong-foot the algorithm and remove cookies, making it think you are somewhere other than where you actually are, or interested in things that actually are of no relevance to you – that it knows very little about you. In a future scenario, the group argued that people have to have control over what algorithms know about you and who that is shared with. The algorithm has to work for the person rather than the person work for the algorithm. An often-used means that we can use to take back control is to set-up different identities and email accounts as a way to separate different areas of your life, e.g. business, personal, shopping. Any future identity system has to respect that people should be able to choose to have separate identities if they want to manage and live their lives in this way.

Future Digital Identity Scheme - Intergenerational Women

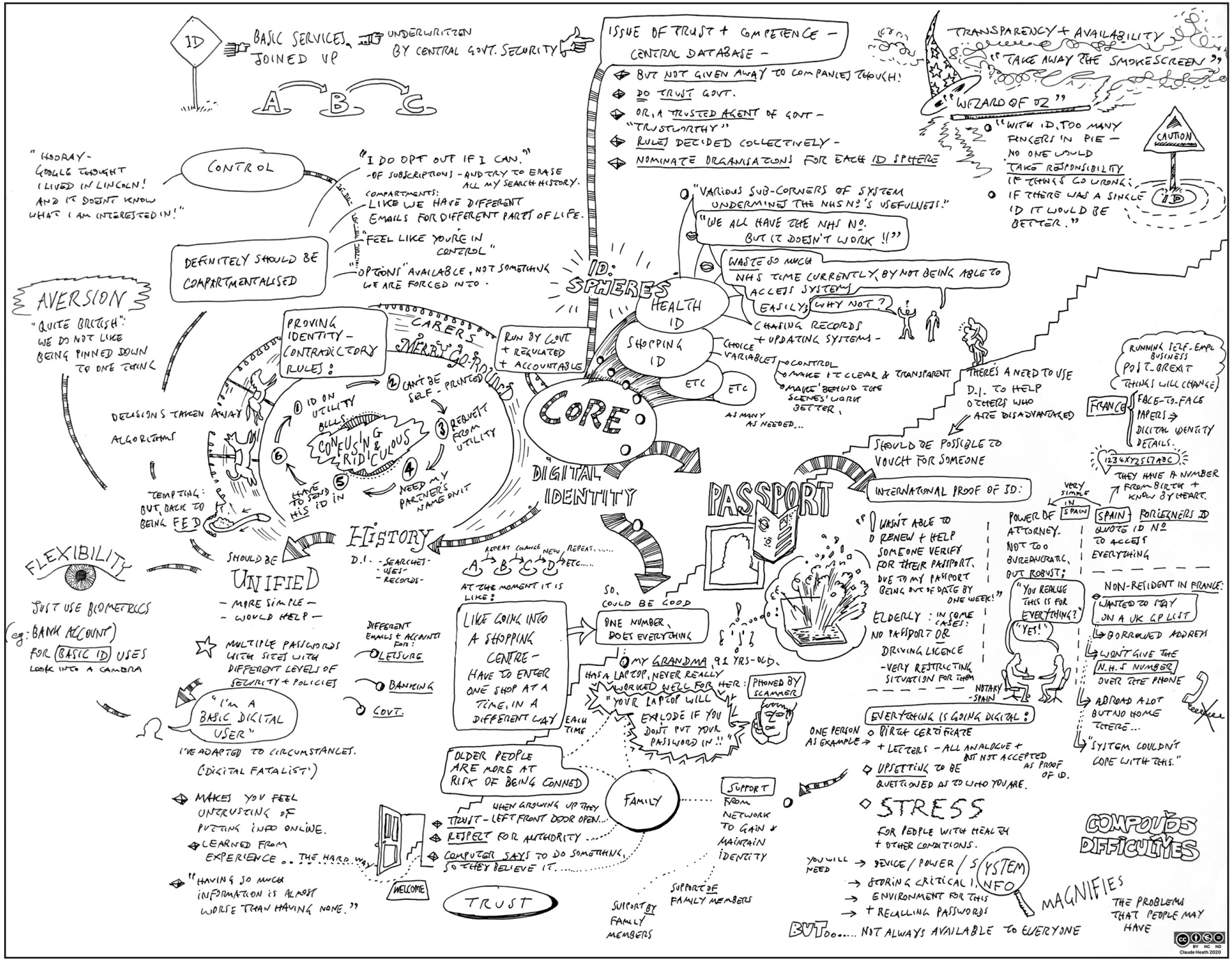
As stated at the start of this section, one possible model is to have a basic identity that everyone has, and this provides access to core services. This basic identity is underwritten by the government and is secured centrally by the government. The government can be trusted to do this because it runs the passport and driver's licence systems. Optional add-on identity modules can be added to this basic identity, to cover the different spheres of people's lives, shopping being one example given. These add-ons may be run by trusted agents but the governance rules for those agents should be collectively decided and defined with the identity agents being fully accountable to those rules. The rules and algorithms have to clearly and transparently be seen to work for people, rather than the other way around.

Visual Note:

In the visual note on the next page, an identity that was core is placed at the centre of the note. Visually it is striking that the core identity becomes central to so many activities. It is also noticeable that the type of identity that you have controls what you have access to and therefore how you are seen by the system. How this picture is interpreted depends entirely on who has control. If third parties and the government have control and are not accountable to the identity holders, then this becomes a picture of barriers and challenges. If the identity holder has control, then this becomes a picture of possibilities and empowerment.

x

Please see page 5 for the full drawing by Claude Heath.


ID
BASIC SERVICES JOINED UP
A B C
UNDERWRITTEN BY CENTRAL GOVT. SECURITY
ISSUE OF TRUST + COMPETENCE – CENTRAL DATABASE –
BUT NOT GIVEN AWAY TO COMPANIES THOUGH!
DO TRUST GOVT.
OR, A TRUSTED AGENT OF GOVT – "TRUSTWORTHY"
RULES DECIDED COLLECTIVELY –
NOMINATE ORGANISATIONS FOR EACH ID SPHERE
TRANSPARENCY + AVAILABILITY
"TAKE AWAY THE SMOKESCREEN"
"WIZARD OF OZ"
"WITH ID, TOO MANY FINGERS IN PIE – NO ONE WOULD TAKE RESPONSIBILITY IF THINGS GO WRONG; IF THERE WAS A SINGLE ID IT WOULD BE BETTER."
CAUTION
"HOORAY – GOOGLE THOUGHT I LIVED IN LINCOLN! AND IT DOESN'T KNOW WHAT I AM INTERESTED IN!"
CONTROL
"I DO OPT OUT IF I CAN." – OF SUBSCRIPTIONS – AND TRY TO ERASE ALL MY SEARCH HISTORY.
COMPARTMENTS: LIKE WE HAVE DIFFERENT EMAILS FOR DIFFERENT PARTS OF LIFE.
"FEEL LIKE YOU'RE IN CONTROL"
"OPTIONS" AVAILABLE + NOT SOMETHING WE ARE FORCED INTO.
DEFINITELY SHOULD BE COMPARTMENTALISED
"VARIOUS SUB-CORNERS OF SYSTEM UNDERMINE THE NHS No.'S USEFULNESS."
"WE ALL HAVE THE NHS No. BUT IT DOESN'T WORK !!"
WASTE SO MUCH NHS TIME CURRENTLY BY NOT BEING ABLE TO ACCESS SYSTEMS EASILY; WHY NOT?
CHASING RECORDS + UPDATING SYSTEMS –
ID SPHERES
HEALTH ID
SHOPPING ID
ETC
CHOICE VARIABLE
AVERSION
"QUITE BRITISH": WE DO NOT LIKE BEING PINNED DOWN TO ONE THING
PROVING IDENTITY – CONTRADICTORY RULES!
CARERS
MERRY-GO-ROUND
RUN BY GOVT. + REGULATED + ACCOUNTABLE
CORE
1 ID ON UTILITY BILLS
2 CAN'T BE SELF-PRINTED
3 REQUEST FROM UTILITY
4 NEED MY PARTNER'S NAME ON IT
5 HAVE TO SEND HIS ID IN
6
CONFUSING & RIDICULOUS
DECISIONS TAKEN AWAY
ALGORITHMS
TEMPTING: BUT, BACK TO BEING FED
DIGITAL IDENTITY
HISTORY
D.I. – SEARCHES – USES – RECORDS –
AT THE MOMENT IT IS LIKE:
A B C D ETC.....
REPEAT CHANCE NEW REPEAT.....
SHOULD BE UNIFIED
– MORE SIMPLE –
– WOULD HELP –
SO, COULD BE GOOD
ONE NUMBER, DOES EVERYTHING
LIKE GOING INTO A SHOPPING CENTRE – HAVE TO ENTER ONE SHOP AT A TIME, IN A DIFFERENT WAY
EACH TIME
FLEXIBILITY
JUST USE BIOMETRICS
(eg: BANK ACCOUNT) FOR BASIC ID USES
LOOK INTO A CAMERA
MULTIPLE PASSWORDS WITH SITES WITH DIFFERENT LEVELS OF SECURITY + POLICIES
DIFFERENT EMAILS + ACCOUNTS FOR: LEISURE, BANKING, GOVT.
"I'M A BASIC DIGITAL USER"
I'VE ADAPTED TO CIRCUMSTANCES. ('DIGITAL FATALIST')
MAKES YOU FEEL UNTRUSTING OF PUTTING INFO ONLINE.
LEARNED FROM EXPERIENCE .. THE HARD WAY
"HAVING SO MUCH INFORMATION IS ALMOST WORSE THAN HAVING NONE."
MY GRANDMA 91 YRS-OLD. HAS A LAPTOP, NEVER REALLY WORKED WELL FOR HER: "YOUR LAPTOP WILL EXPLODE IF YOU DON'T PUT YOUR PASSWORD IN!!"
PHONED BY SCAMMER
OLDER PEOPLE ARE MORE AT RISK OF BEING CONNED
WHEN GROWING UP THEY
TRUST – LEFT FRONT DOOR OPEN...
RESPECT FOR AUTHORITY ...
COMPUTER SAYS TO DO SOMETHING, SO THEY BELIEVE IT.....
WELCOME
FAMILY
TRUST
SUPPORT BY FAMILY MEMBERS
SUPPORT OF FAMILY MEMBERS
SUPPORT FROM NETWORK TO GAIN & MAINTAIN IDENTITY
THERE'S A NEED TO USE D.I. TO HELP OTHERS WHO ARE DISADVANTAGED
SHOULD BE POSSIBLE TO VOUCH FOR SOMEONE
AS MANY AS NEEDED...
CONTROL
MAKE IT CLEAR & TRANSPARENT
MAKE 'BEHIND THE SCENES' WORK BETTER.
PASSPORT
INTERNATIONAL PROOF OF ID:
WASN'T ABLE TO RENEW + HELP SOMEONE VERIFY FOR THEIR PASSPORT, DUE TO MY PASSPORT BEING OUT OF DATE BY ONE WEEK!
ELDERLY: IN SOME CASES: NO PASSPORT OR DRIVING LICENCE – VERY RESTRICTING SITUATION FOR THEM
EVERYTHING IS GOING DIGITAL:
ONE PERSON AS EXAMPLE →
BIRTH CERTIFICATE + LETTERS – ALL ANALOGUE + BUT NOT ACCEPTED AS PROOF OF ID.
UPSETTING TO BE QUESTIONED AS TO WHO YOU ARE.
STRESS
FOR PEOPLE WITH HEALTH + OTHER CONDITIONS.
YOU WILL NEED → DEVICE / POWER / S
→ SECURING CRITICAL I.
→ ENVIRONMENT FOR THIS
→ + RECALLING PASSWORDS
SYSTEM INFO
BUT... NOT ALWAYS AVAILABLE TO EVERYONE
MAGNIFIES THE PROBLEMS THAT PEOPLE MAY HAVE
COMPOUNDS DIFFICULTIES
NOTARY – SPAIN
"YOU REALISE THIS IS FOR EVERYTHING?"
"YES!"
POWER OF ATTORNEY. NOT TOO BUREAUCRATIC, BUT ROBUST:
VERY SIMPLE IN SPAIN
SPAIN
FOREIGNERS ID
QUOTE ID No. TO ACCESS EVERYTHING
NON-RESIDENT IN FRANCE:
WANTED TO STAY ON A UK GP LIST
BORROWED ADDRESS
WON'T GIVE THE N.H.S NUMBER OVER THE PHONE
ABROAD A LOT BUT NO HOME THERE...
"SYSTEM COULDN'T COPE WITH THIS."
RUNNING SELF-EMPL BUSINESS POST-BREXIT (THINGS WILL CHANGE)
FRANCE
FACE-TO-FACE PAPERS → DIGITAL IDENTITY DETAILS.
1234XYZ567ABC
THEY HAVE A NUMBER FROM BIRTH + KNOW BY HEART.
Claude Heath 2020