

Smartphone as Lifeline: Designing Technology for a Changing World

AUTHORS: STEPHANIE HANKEY, CADE DIEHM, ROSE REGINA LAWRENCE AND MAREK TUSZYNSKI

**TACTICAL
TECH**



Introduction

BY STEPHANIE HANKEY

The global community is undergoing unprecedented political, environmental and social changes. In this context, smartphones provide essential access to resources, services and vital connections to friends and family, either temporarily or in an ongoing way. This research study asks: How can we design data-driven technologies for the real world, not the ideal world?

The core functions of smartphones have become normalised. They are now extensions of the self, allowing us to move through digital environments seemingly with ease and to an increasing extent, as Lovink states, as emotional support devices to which we are habituated. Whether we value them for passing time or self expression, we also rely on them practically to a greater and greater extent; for coordinating with others and getting around, discovering information about or controlling our environments, or utilising them as identifiers, ‘passports’, ‘tickets’ or ‘credit cards’. Smartphones have become the Swiss Army knife of day-to-day life: the one thing you cannot leave home without.

However, what would it mean to design smartphones not as consumer goods – for shopping, finding a restaurant or controlling your other smart devices – but rather as essential lifeline devices? Through a process of literature review, research and analysis, this paper outlines what design principles and factors would need to be considered if smartphones were to be designed for those who use them for support, services and survival.

For those living in vulnerable, disadvantaged or transitional contexts, smartphones are essential. Our review highlights that when people have restricted access to funds, unstable environments, and poor internet reliability or disrupted access it does not reduce the value or central importance of smartphones. On the contrary, living in precarious, shifting and volatile contexts may even increase the value of such tools – acting as an indispensable means of communication for safety, coordination and survival. They are also **‘gateway devices’** – a central means through which almost all other resources can be accessed. As such, they are also devices that can amplify vulnerabilities. These new forms of dependency simultaneously create new sites of struggle; assets which become open to inequitable exposure, control and manipulation. In vulnerable contexts, whether temporarily or over a longer term, smartphones are often a lifeline but they can also be a liability because of the way they are currently designed.

Throughout this study, the different levels of computing – society, infrastructure, data, device – are continuously referenced. As smartphones become a central interaction device for all other applications, devices and sensors, this becomes increasingly unavoidable.

The first part of the paper, ‘Smart Technologies and Precarity’ examines how personal technologies are currently utilised by and for communities living in precarious situations. In particular, we focused on people living through natural disasters or in crisis situations, refugees and migrants and those living in poverty. We have chosen to have a greater focus in this overview on the Global North out of recognition that such precarity is normally studied in the Global South¹ and that there is a distinct lack of synthesis of information on how this impacts communities in other parts of the world, such as North America and Europe. The terms ‘Global North/Global South’ and their definitions are imperfect but we have chosen to use them here in guiding our research to flip assumptions that disaster, poverty, migration and disadvantage is more prevalent in the Global South¹. It is our observation that much can be learned and more opportunities for solutions may be found if these issues are recognised as truly global challenges with increasingly fewer differences between regions.

The second part of the paper, ‘Identifying the Issues’ looks across communities and groups and identifies four common themes that are currently under explored when designing for such contexts. These are identified as: 1. *dependency* – in what ways do personal technologies act as an essential lifeline? 2. *identity* – how are digital identities currently formed through personal devices and related technologies, such as biometrics? 3. *agency* – what is the user’s experience of control over and choice related to their devices and how does this relate to social and cultural power dynamics? and lastly 4. *multipliers* – what are the other dimensions, such as changing circumstances over time and scale of solutions, that can exacerbate problems and should impact design decisions?

“The mobile has come dangerously close to our psychic bone, to the point where the two can no longer be separated.”

GEERT LOVINK, SAD BY DESIGN

This study does not attempt to be a comprehensive review of this vast and overlooked area in technology design and the ethical questions ‘smartphone as lifeline’ brings. Rather it lays down essential foundations for bringing existing issues and associated literature together and sets the scene for necessary work going forward. It is intended as a conversation starter about designing for difference and for disadvantage and an invitation for different stakeholders – from civil society and community groups to public and private sector practitioners, decision makers and influencers – to take these points forward into meaningful review and reflection that leads to action.

We have framed our analysis neither as for nor against technology use in these contexts, but rather treat it as an inevitable development. We see the use of personal devices in such contexts as desperately requiring more research in order to develop a deeper understanding of needs, investment of time and energy in order to ensure that we have design models and methods that work for ‘society as user’ not just individual users. There is also a need for increased capacity building for governments, regulators, funders and civil society groups to help them engage in the political, social and cultural challenges brought by the widespread integration of and dependency on such technologies.

Whilst the majority of this research was undertaken between 2018 and 2019, the more recent widespread use of mobile phone technologies to track and trace the spread and control of Covid-19 has further shown how essential personal devices are for mitigating, solving and supporting global problems for a vast range of communities. The current activation of these technologies and associated data in such a wide range of contexts in response to a worldwide pandemic makes this research all the more poignant. Now, more than ever, we need to understand how technology works not only as an enabler but also as a magnifier, and the trade-offs it forces us to make.

As the designer and educator Victor Papanek advocated in 1972, we need to learn to design for the ‘real world’ not the ‘ideal world’. In the current moment, we urgently need design methods that enable all stakeholders to develop technologies which recognise the real life scenarios of our ‘changing world’.

Part I: Smart Technologies and Precarity

This study recognises that users living in precarious, vulnerable or rapidly shifting situations are disproportionately exposed to increased risk through their use of certain smartphone-based operating systems (OS), platforms, applications and ecosystems of connected devices. These technologies reach many populations who lead lives drastically different from the populations of designers and developers most actively building them. For this reason it seeks to scope out some of their challenges and invite more rounded, diverse and holistic approaches to technology design in the future. In addition, this study seeks to examine how users may be further impacted by future design principles, such as how smartphones and related technologies treat core functions like identity, control, access, permanence, data and how these can interact with the core functions of devices and their built-in sensors.

Smartphones are now ubiquitous. An estimated 6 billion devices are in circulation in 2020², each running one of only a handful of operating systems. Although the most successful operating systems are intended for ‘universal access,’ there is a wide range of users who are dependent on smartphones and whose experiences are significantly more complex and poorly understood, globally: For example, people experiencing crisis or disaster situations, migrants, refugees or asylum seekers, or more routinely, people living in poverty and low-income communities. The goal of ‘universal access’ inherent in smartphone design frequently fails individuals and communities across many examples of change. We found that across these varied communities there are a range of shared difficulties and failings in the relationship between users and their smartphones.

Most attempts to understand the impact of disadvantage and vulnerability on smartphone use has focused to date on communities in the Global South, where smartphones are sometimes researched in terms of dependencies but largely studied in the context of introducing educational and economic opportunity. In the Global North, however, recent efforts to understand challenges of smartphone use have focused more on the notion of “digital well-being,” in particular users’ relationships with their phones in the context of habituation, control and addiction. It is our hope to extend both of these horizons. We believe digital well-being could be understood in a much broader framework. This term could not only refer to users’ habits and their individual relationship with technology but also the overall well-being of the user in a context where smartphones are essential gateway devices and increasingly extensions of the self.

There is a distinct lack of ‘deep’ research about how smart devices are utilised in the Global North by communities in need, in particular with regards to the challenges of technology design. This leads to assumptions in designing for different markets. One example of this is the mistaken belief amongst technology makers we interviewed that users with a lack of access to resources – such as low-income communities – would forego their paycheck or food for access to a high-end device because of social or aspirational status. Our research through workshops suggests that this ‘consumer lens’ overlooks the critical role that smart devices also play in their lives and the wisdom that cheap does not often mean durable. Low income communities may make sacrifices to pay for an expensive phone, this may be aspirational but it is also symbolic due to its essential function in their lives, such as access to work, money and services and the ‘emotional role’ of the smart device: the woman using the phone to get through a part of the city safely at night, the single parent staying in touch with caregivers whilst they are at work, and so on.

Because of the lack of research in this specific area, we undertook some interviews with technology designers, community researchers and collaborators. These interviews helped to form our questions, frame the literature review and fill in gaps in found knowledge. However, the majority of our study is formed of journal articles, tier-one media, newspaper reports and non-profit and industry reviews. We have also utilised and referenced a range of academic research papers. Whilst some scholars, writers and activists write more extensively about the challenges of smartphone use by vulnerable and disadvantaged communities in the Global North, very few of them approach this from a technology design perspective.

Smartphones and other data-driven technologies used for those living in precarious situations

For the purposes of this study we focused on three marginalised and vulnerable communities that rely on smartphones and other personal devices and share a common factor, which is the transient and unstable nature of their circumstances. They are each subjected to temporary or prolonged shifts that can significantly influence their situation suddenly, unpredictably and beyond their control. For these reasons, we refer to these contexts as precarious situations. Precarity, as defined by Isabel Lorey, means “living with the unforeseeable, with contingency.”³ Whether self-identified or not, we have referred to these groups and clusters of individuals as communities due to commonalities amongst their situations, not because they themselves necessarily see themselves as part of a particular community.

The groups and contexts we chose to focus on were:

- 1) living through disaster or crisis situations;
- 2) refugees, migrants or displaced persons; or
- 3) living in poverty or experiencing economic precarity.

The nature of the circumstances in which these communities find themselves may also affect the urgency, level of risk and varying investment of time, money and resources that people within these groups are willing to make in their smartphone use. For example, those living through a disaster may be subject to a radical yet relatively temporary change where the focus is on rebuilding and reconnecting their lives, as opposed to refugees and migrants who may be in a longer-term transition.

Disaster and Crisis Situations Smartphones as a source of warning, connection and response, providing a lifeline before, during and after a crisis.

Smartphones have become key resources in disaster and crisis situations. They are both a source of information and a lifeline before, during and after a disaster. The rate of smartphone use is so high during disasters and crisis situations that mobile phone providers have used the sudden widespread spike in activity to observe moments of crisis before news outlets are able to report on them.⁴ In recent cases this has caused the only known instances of network overload,⁵ indicating how important phones have become in disasters. Studies have shown that over 70% of Americans use phones to keep track of breaking news events.⁶ This figure from 2015 is likely to have increased steadily along with the growth curve of smartphone and mobile app penetration in the US.

The potential for technology use in disaster situations has led to an expanding field of study and development, including:

- prediction, modelling and early warning systems⁷
- sensors and social media listening
- news, apps, alerts, warnings and advice for those caught in a disaster
- alarms and SOS calls
- rescue and relief effort coordination (in particular to help first responders understand where to go, what to do and what the priorities are)
- information-sharing and coordination between agencies and across borders
- longer-term rehabilitation efforts post-disaster
- tracking and tracing human mobility
- management and control of disaster and crisis situations

A significant and growing technology sub-sector has emerged in response to this recognised potential. For example, in 2012, the Federal Emergency Management Agency (FEMA) hired its first Chief Technology Officer. There are also a wide variety of corporate social responsibility programmes,⁸ conferences, trainings and events (such as the recent Silicon Valley-area conference on relief technologies);⁹ and start-ups working on apps, sensors, drones,¹⁰ robotics,¹¹ autonomous vehicles¹² and even smart harnesses for rescue dogs.¹³

There is a high degree of innovation and research in this sector, including proposals for possible systems for first responding, disaster surveillance or resilient emergency communications,¹⁴ but only few have been implemented at scale. Despite this, the US is a field leader alongside a number of countries in the Asia-Pacific region – in particular Japan, the Philippines and Australia. This is due to the scale and severity of recent disasters and the prevalence of local technology infrastructure. In November 2019, Australia experienced the worst fires in the country's history across multiple states. This was met with significant development of new mobile apps that include real-time reporting of fire movement and air pollution.¹⁵ Similar tools are available in California and other fire-prone regions.

Beyond innovation, the collisions of existing digital infrastructure and the impact of disaster are poorly understood. For example, algorithmically-powered traffic routing apps that favour traffic-free areas may accidentally guide unsuspecting motorists into early-stage fires, where evacuation is mistaken for a lack of road congestion,¹⁶ generating a 'preferred' but deeply undesirable route.

From the very start of the Covid-19 pandemic that took hold worldwide in early 2020, mobile phones were considered a central part of the governmental and public health response, from modelling and understanding the spread and movement of the virus to finding methods to trace, track, manage and control its spread. Examples of mobile phone location data use emerged early on in Asia but quickly moved to Europe, with operators in Italy, Austria and Germany sharing their data with the government to learn more about the spread of the virus.¹⁷ A wide range of technologies have sprung up in this context, many of them using geo-location data from smartphones but some utilising proximity data from Bluetooth. In addition, mobile phones have also been utilised to get health related messages to citizens

and to warn them when they are leaving their area and breaking the rules and regulations of lockdown, such as Poland's quarantine enforcement app.¹⁸ So many emerged in the first few weeks in response to the spread of Covid-19 that groups such as Privacy International began a dedicated resource to track the developments across countries.¹⁹

Migrants, refugees and asylum seekers
Smartphones as connectors, way-finders and passports, helping refugees to bridge the contexts of where they came from and where they are going.

Sixty-eight million people in the world are currently displaced – more than during the Second World War.²⁰ The number of migrants and displaced persons is predicted to increase in the next 30 years, with the World Bank anticipating that over 140 million people will be forced to migrate due to climate change by 2050.²¹ In such situations, smartphones are essential for individuals and families.²² This has been particularly notable in the recent refugee crisis, with a dedicated academic field emerging known as 'digital migration studies'. Mobile phones are widely thought of as being 'the social glue of migrant transnationalism'.²³ A UNHCR and Accenture research study conducted in 44 countries found that many refugees consider mobile and internet access as critical to their safety and security as food, water and shelter. Refugees often spend up to a third of their disposable income on internet and mobile services, which reflects that staying connected is expensive, but also indispensable.²⁴ One study puts it simply in this quote from a refugee: "It is hard to think of a more useful thing to own than a smartphone, especially if you're fleeing your home."²⁵

The last few years have seen the idea of the 'connected migrant'²⁶ emerge. Alongside this have come a host of allegations about 'false' refugees arriving, often judged by the fact that they are carrying the latest smartphone.²⁷ This has done little to aid prejudice but has dispelled myths that refugees are predominantly poor and technologically illiterate. Whilst there are a variety of types of refugees, researchers widely agree that across diverse groups, they are still relatively tech-savvy. In Europe the majority of asylum seekers are men under 30, contrasted against the smaller proportion of women – the majority of whom are over 65.²⁸

Smartphones are equally an essential information source for relief agencies, where they assist displaced persons and supporting authorities in tracking the scale of displacement and migration.²⁹ The importance of technology to this community has been so significant that, as with the disaster and technology sector, there have been a wide variety of technological developments.³⁰ An existing community of app and technology makers – some of whom are refugees themselves – are seeking to support the development of smartphones for this group, from ways to navigate train systems to apps for Syrian refugees to navigate German bureaucracy.³¹ This includes dedicated events for technologists, for example the Techfugees Global Summit held in Paris in October 2018.³² There are currently over 700 apps that have been developed specifically for refugees, many of which have few to no users. This has led to some words of caution from relief agencies about the enthusiasm of tech developers rushing in to help without really understanding the practical, social, psychological or political dynamics of this community. Well-meaning time is often spent developing solutions that don't work, aren't appropriate or connected to the communities in their roll-out, and in some cases may exacerbate and compound problems. However, some that are significant and helpful have emerged, mostly developed in collaboration with humanitarian organisations.³³

As useful as smartphones are to refugees and migrants, there is also widespread recognition that 'digital passages' create new vulnerabilities, inequities and potential for manipulation, misinformation and abuse. Threats come from a number of different actors, creating "socio-technical spaces of flows in which refugees, smugglers, governments, and corporations interact with each other and with new technologies."³⁴ For these reasons, dependency comes with a range of ethical and safety considerations. Smartphones are lifelines that pose risks in that the data traces they produce can also lead to ongoing scrutiny,³⁵ as exemplified by the rise in mobile forensic data technologies used by border and law enforcement agencies.³⁶

Poverty and low-income communities
Smartphones as enablers for work, mobility and safety.

In December 2017, the UN special rapporteur on Extreme Poverty and Human Rights, Philip Alston, launched an investigation into extreme poverty in the US.³⁷ His report

“Smartphones are lifelines that pose risks in that the data traces they produce can also lead to ongoing scrutiny”

found that in one of the richest countries in the world, 40 million people are now living in poverty. This was followed by a parallel investigation in the UK in August 2018, with a particular focus on how Brexit will affect poverty. In the UK, the Joseph Rowntree Trust estimated that 14.2 million people were currently living in poverty, meaning approximately one in every eight people.³⁸ In the US, there were 31.8 million people living in poverty around the same time.³⁹

Significant studies have shown that usage patterns of mobile phones for those living below the poverty line are different from those living above it.⁴⁰ A Pew Study published in 2017 and updated in 2019 showed that smartphones in America were a primary asset in low-income families. It found that in terms of economic commitments, a stable home internet connection and laptops were viewed as less vital than smartphones and data. The same study also found that there are significant differences by race in low-income communities.⁴¹ A wide range of studies further echo this, confirming that “... differences in smartphone dependence and use based on race, age, income, and education exist. Minority group members, younger, lower income, and less educated users are more likely to be smartphone-dependent.”⁴²

Smartphone users living in poverty are disproportionately likely to use older smartphones running operating systems that are no longer supported by vendors. Out-of-date hardware and operating systems can cause harm to the user – the further away a user is from the newest operating system and modern secure hardware, the more problems arise with security and functionality. ‘Software rot’ is directly linked to socio-economic status, and this dynamic creates a cycle of further entrenched disadvantage, as often older devices owned by such communities can’t cope with system updates. The close linking of smartphone hardware with features like biometric authentication via newer sensor hardware, or reliance on additional secure hardware (such as the Secure Enclave⁴³, TrustZone⁴⁴ and Titan M⁴⁵) illustrates the differences in security over generations of smartphones. This is further compounded by community suspicion of software updates as vehicles planned for obsolescence, in which subtle but deliberate sabotage of devices and operating systems are introduced by carriers or vendors to encourage hardware upgrades.⁴⁶

More recent widespread use of mobile phones for tracking and tracing in response to Covid-19 has also shown that there is a direct link between the age of a

‘Software rot’ is directly linked to socio-economic status, and this dynamic creates a cycle of further entrenched disadvantage, as often older devices owned by such communities can’t cope with system updates.

device and the ability to utilise and take part in certain systems. The tracing technologies that were designed through an unprecedented collaboration between Apple and Google in early 2020 relied on a technology that is absent from an estimated 2 billion phones,⁴⁷ many of which are owned by people in low-income communities. This is a double-edged sword, where some advocates would say that being left out of from such a scheme is a major discrimination, whereas other privacy advocates may see this as a distinct advantage.

As with the refugee community, overexposure of data is a significant issue for low-income communities and those living in poverty. Overall, low-income communities have the most data collected on them – offers for cheap data plans, or loyalty vouchers, etc. – in return for free or automated services and surveillance from authorities and law enforcement. In cases where this appears voluntary, often consent is given at the behest of economic or social vulnerabilities. Virginia Eubanks dispels the myth that people living in poverty in the US are also living in ‘technological poverty’, showing that they are frequent users of technology on a daily basis, either directly through their own devices or indirectly through technologically-mediated services. Eubanks identifies the real problem of poverty and technology as the rise of the ‘digital poorhouse’.⁴⁸ The profiling, scoring, rating and permanent tracking of individuals living in poverty creates and compounds discrimination, leading to cumulative disadvantage⁴⁹ – an ongoing cycle of poverty and debt that makes it harder to escape.

Other communities with high smartphone and smart device dependencies

Alongside these three main communities, we also undertook a preliminary round of research looking at communities who are for different reasons dependent on devices, and are identified by challenges they face because of their gender, ability and age. A brief overview of these groups includes:

Women living in precarious situations: Women living in precarious situations are often dependent on both smartphones and IoT devices. At the same time, these devices expose them to heightened risks from the sources of their precarity. For example, women living in or escaping from a domestic violence situation rely heavily on smartphones for their wellbeing and safety. This can serve to break isolation, maintain contact with

friends and family, and enable individuals to get access to information and services. One example that could be adapted is ‘panic button’ IoT, where features are designed within smart devices to discreetly connect a user in distress to help. This is already being trialled in hotels, to protect housekeeping staff.⁵⁰ At the same time, devices can also be controlled, subject to surveillance and spyware from partners, and can lead to escalation of physical violence.

Elderly living in precarious situations: The elderly are increasingly accessing public services through tablets (with a lower learning curve than computers or smartphones) and due to a growing trend toward ‘ageing in place’ solutions⁵¹ they (and their carers) increasingly use IoT sensors and other smart devices that are then often connected to carers smartphones through an app – or as it is sometimes referred to, ‘IoT for the Golden Years’. This creates opportunities for extending care remotely and increasing safety and wellbeing, but also significantly decreases agency, providing other family members and carers with the ability to control and access devices remotely. There is also an increase in care and elderly homes introducing sensors and personal devices for monitoring well-being.

Youth living in precarious situations: One in five of all internet users in Europe are under the age of 18.⁵² Youth are therefore an important sub-user group when thinking of any community needs. Within the core communities of this study, they are also active users and often act as ‘infomediaries’ for others. This is particularly the case for refugees, migrants and those living in poverty. Younger people can act not only as go-betweens, but also as ‘digital natives’ in their communities, who can set up devices, maintain them and share skills with others.⁵³

People with disabilities living in precarious situations: People living with disabilities are increasingly reliant on smart devices tied to their smartphones, both in the home and in terms of mobility. Smartphones and IoT devices can be enablers: augmenting abilities and reducing barriers; extending opportunities for communication and coordination with others; providing access to support and healthcare; and expanding access to education and work. However, they also can compound differences, reinforce isolation and extend power dynamics with carers. There is a significant overlap between disabilities and those living in poverty. The Rowntree Trust’s 2017 study found that nearly

half of those locked in poverty in the UK (6.9 million people) have disabilities or are caring for those with disabilities.⁵⁴

LGBTIQ living in precarious situations: Within the LGBTIQ community, precarity presents itself in a different way; the invisibility of sexual minority (eg closeted) in some contexts drives a dependency on networks of ephemeral interaction, and online moderated spaces of support and self-built community. The political framework of queer visibility leads to an embrace of vulnerability in the face of discrimination in many cases. Despite the recent gains in queer acceptance in mainstream liberal democracies, a structural lack of online privacy is leveraged by opponents of LGBTIQ rights⁵⁵ and queer individuals (and their allies⁵⁶) often face threats, harassment, doxxing or physical harm.^{57 58 59 60} Visibility through geo-location, such as smart phone-dependent dating apps,⁶¹ is also used to seek partners or intimate connections online. The increasing reliance on these platforms – particularly location-based dating services – offers both additional safety (for example, moving an online date into the real world and being watched over by a trusted friend) whilst also heightening risks for physical safety, in which a potential date can use multiple data points to discover personal information about an individual that might not be otherwise shared in an offline date.

The wealth of data generated by queer individuals online includes sexual health statistics, selfies as politics, and social graphing of queer communities. The amount of data that is available online makes these communities vulnerable to profiling and to experiments, such as using facial recognition and algorithms to infer whether an individual is gay.⁶²

Ethical questions for technology dependency and vulnerable and marginalised communities

Whilst some of the technology-related solutions and challenges for each of these different communities and contexts are summarised above, we found that there were many commonalities between them. These factors are important as they make the case for more advanced conversations around notions of consent and informed choice as well as an increased need for transparency and ethical review. Such questions are explored further and through particular themes in the next section, where we

picked up just four of the many themes that emerged from our literature review and explored them in more detail.

Whilst the groups and communities outlined above are described separately, there are many interlinkages between them, especially as some individuals can fit into more than one of these categories above. For example, people living in a low income community could experience a natural disaster, and this can significantly extend dependencies and compound inequities.

From the technology solution perspective, we have also seen that technologies developed in one context with one community or problem in mind can lead to innovation or reapplication in another context. In some situations this cross-issue application of technology can lead to quick innovation and effective learning through testing and development of solutions. However, in other contexts it can pose new challenges. In particular, there is a danger that in some cases technologies can be first tested in communities with less voice and where there are less tightly enforced regulatory frameworks. This can raise ethical questions as tools that infringe on privacy or reduce agency are at times tested on those with the least agency and the least power. For example, in early 2020 the Bureau for Investigative Journalism published a study by Crofton Black that explored the interlinkages between technologies tested on migrants for tracking and identifying refugees that were then used for tracking and tracing Covid-19.⁶³

Further research in this area should seek to work across issue areas, understanding technology challenges as requiring an intersectional approach. More precisely, this means greater collaboration is needed across civil society sectors and issue areas when working with technologists. Cross-sectoral collaboration is necessary in order to understand how technologies are tested across sectors, for example how technology for tracking the movement of migrants can be used for tracking human mobility in public health outbreaks, as highlighted above. Cross-sectoral collaboration could both lead to better identification of effective solutions, best practices and ethical interventions but also create mechanisms for identifying civil liberties, surveillance and human rights implications that need to be addressed.



Part II: Identifying the Issues

Common themes

When examining the needs and challenges of vulnerable communities and smartphone dependency, clear themes emerge that can be extrapolated in order to carry out a cross-sectional analysis. A thematic rather than sector-driven approach can help identify more powerful solutions rather than niche products. It can also lead to more fundamental philosophical technology design shifts that could be adapted over time as needs, circumstances and situations change and as technologies shift and develop. In order to lay the groundwork for this way of understanding designing for difference, we specifically chose four themes we found that were common across the communities we researched, yet very little analysis exists to date that brings together these issues within the context of smartphone use by vulnerable and disadvantaged communities.

The core themes we identified through this landscaping and literature review are:

- **Dependency: Smartphones as ‘gateway devices’**
 - *Lifeline: Access to a reliable device*
 - *Continuity: The challenge of maintained access*
 - *Resources: Using vital services*
- **Digital Identities: The myth of “one person, one device”**
 - *The individual: The fractured digital self*
 - *Groups and relationships: How identity is used by others*
- **Agency: Inherent vulnerabilities in dependency**
 - *Power relations: Amplifying real-world structures*
 - *Control: Trade-offs between automation and choice*
- **Multipliers: Thinking about variables**
 - *Time: A key factor in precarious living*
 - *Design: Principles for millions of individuals*

1. Dependency

Smartphones as ‘gateway devices’

Dependency on smartphones is a key factor for communities living through disasters, migrants and refugees or communities living in poverty. Dependency here is understood not as a question of habit or addiction, but rather as a critical relationship with a phone as a way of getting vital access to resources and impacting a user’s fundamental freedoms (identity, mobility, rights etc). This means that smartphones act as ‘gateway devices’, providing access to essential elements through which everything else can be accessed; from access to up-to-date information, to shelter, money, healthcare and support.

Dependency has been divided into three aspects: a. lifelines, b. continuity of access and c. access to essential resources.

Lifeline

Access to a reliable device

Smartphones often act as a ‘lifeline’ for people on the move and for those living in poverty. For this reason, reliability and durability as well as continuity of access through a ‘gateway device’ are essential factors. We have called this section ‘lifeline’ as it is the baseline around which all other factors revolve: without a working smartphone, all the other considerations become less relevant. For all the groups in our research, this creates a high degree of stress for users and the need to generate extra work-arounds to manage and maintain devices.

There are four aspects that are central to the ‘lifeline’ of smartphones. These are:

- *Battery life and energy efficiency*
- *Connectivity, cost and supply of data*
- *Usability of the device itself (i.e. can it be reused, recycled, adapted, replaced, shared?)*⁶⁴
- *Access to broader infrastructure, for example a mobile phone signal*

There are a wide range of work-arounds to try to maximise energy efficiency and extend battery life, from portable battery charging devices to user-shared tips on minimising power use in times of need.⁶⁵ This is particularly the case for users on the move or with infrequent, intermittent or unreliable access to power. More work could be done to find solutions to this rudimentary problem, including smart solutions at the OS level.

The same is true of questions of connectivity and data use: much research attempts to understand these challenges concretely in the Global South context.⁶⁶ But even tackling something as seemingly straightforward as connectivity and data usage may have its challenges for some communities. For example, in low-income communities, smartphone and data usage patterns are increasingly used as proxies for analysing an individual’s ‘reliability’ and ‘trustworthiness’ for access to credit. A very active phone user is considered ‘more likely to be economically active’.⁶⁷

Recycled and reused phones are commonplace for communities living in poverty, such as those temporarily without sufficient access to finances or those who may have suffered from the loss of a smartphone. For this reason, KaiOS and older versions of the Android operating system are likely the most utilised for the core communities on which this research focused. In the first half of 2019, the most common Android versions used were Android 7.0 and 7.1 (30.8%). The majority of all users, however, are relying on second-hand, low-end devices that use Android versions 6.0 and below. As of October 2018 this constitutes 54% of all Android users.⁶⁸ These versions do not currently receive updates or security patches etc, although this is recognised and is actively being addressed by Google’s Android team.⁶⁹ However, regardless of vendor, the impacts of unsupported operating systems can be significant to our priority communities as these unpatched systems are more open to vulnerabilities and abuse. Of particular note is the extension and growth of this market: whilst some communities are leap-frogging and starting from recent versions of the OS, others are relying on a burgeoning refurbishing and re-branding industry,⁷⁰ with distinctive business models in the most rapidly growing regional markets, in particular South-East Asia (most notably China and India) and Africa.

Access to mobile phone networks is a major factor in rural areas and for the rural poor. However, sudden loss of infrastructure, in particular in disasters, creates difficulty in using devices. For this reason there is currently some innovation surrounding emergency mobile phone tower provision and other forms of access.⁷¹ The essential nature of mobile phones during a disaster is further indicated by the range of existing programmes by mobile device manufacturers and mobile network providers, including initiatives by Ericsson⁷² and Vodafone⁷³ and in cases such as in El Salvador, where providers provide zero rating (access to certain apps or websites with no data charges) during disasters.⁷⁴

Continuity

The challenge of maintained access

A direct follow-on from the core needs identified above is the challenge of continuity of access. The groups highlighted in this study are subject to more vulnerabilities than ‘typical’ users with regards to their devices. Losing access to a working device – whether through loss, confiscation or theft – can be equal to loss of security and safety with immediate and long-term consequences.

For those living in poverty and those who are economically destitute, smartphones are more often subject to ‘theft, loss, breakdown, and regular periods of disconnection due to unaffordable services’.⁷⁵ Fifty percent of people living in poverty and relying on smartphones are not using contracts but rather using minute-based data services, because of the flexibility and control they allow rather than the strain of an additional monthly bill to pay. This is more broadly referred to as the challenge of ‘technology maintenance’. Studies in this area argue that, in an ongoing way, the poor will struggle to maintain digital access after ownership and availability are realised.⁷⁶ This means that owning a smartphone is only one statistic for this community; the question of ongoing and reliable access is another, and one that is not currently measured. For low-income communities and minority groups particularly in the US, civil liberties issues lead to higher rates of phone confiscation, third-party access, surveillance and tracking.⁷⁷

For populations on the move, loss of access, device breakage and theft are significant challenges. In the case of refugees, theft occurs not because of access to data but to the phone itself as an asset. The principal set of concerns in these cases, when a device is lost or removed, is not necessarily privacy, but rather connectivity with others and the loss of access to resources. For many, the most pressing issues are related to the practicalities of dealing with the loss of a primary tool for connectivity and in particular to backup (system/data, with emphasis on data), access recovery (logins/passwords) or SIM-related (credit, number, services).

Resources
Using vital services

Smartphones are essential as lifelines to individuals and groups largely because of the access they provide. Phones ‘bring people who are close closer together’, increase mobility and facilitate access to vital services such as money and support from others.⁷⁸

Smartphones can be essential resources for all users, regardless of their situation. However, for precarious communities, the stakes may be significantly higher than for a ‘typical’ user, as there may be substantively fewer alternative pathways to resolve challenges. This is particularly acute for disrupted individuals and communities who may temporarily, or permanently, have lost access to their regular environments and belongings; need ongoing information on where to go; require up-to-date information, advice or help; or may need to connect with others for their own safety and the safety of others. This can be broken down as follows:

- Smartphone as connector: Smartphones are an essential tool for finding and staying in touch with family members, friends and contacts, but also for enabling enhanced coordination, and the strengthening and growth of personal networks. In many cases, for our user groups, WhatsApp has become the most important app⁷⁹ due to its widespread use (reported at 2 billion users in 2020),⁸⁰ individual and group messaging features, simple interface and low costs.
- Smartphone as navigation: Smartphones are essential for individuals on the move, in particular for orientation and way-finding, which can include mapping and geographical

information, but also routing, accessing news and up-to-date information and advice. When crossing borders this also includes access to information in native languages and access to trusted and verifiable sources of information.

- Smartphone as safety device: Studies of smartphone use in low-income communities show that these devices significantly enhance daily coordination and safety. ‘Micro-coordination’ describes how users have adopted smartphones and their platforms to address logistical challenges and caregiving (for example organisation via group chat clients); ‘hyper-coordination’ describes how they relate to logistics and safety. Smartphones have been proven to significantly increase movement around urban spaces and therefore have contributed to renewed accessibility of urban spaces.⁸¹ There is often a direct link between mobility and safety in terms of smartphone use, which is particularly true for those living with disabilities.
- Smartphone as access to resources and services: As smartphones are increasingly used for internet access and as state and independent service providers increasingly rely on apps, they have become central to long- and short-term provision of access to public services, immediate and longer-term health and care services, work, housing, and education.
- Smartphone as money: Smartphones are increasingly important amongst our priority communities for:
 - access to credit and funds, especially with the growth of micro-finance schemes and as projects developed under the umbrella of ‘financial inclusion’ become more prevalent outside the Global South.
 - access to income and labour – as devices become the primary facilitator of ‘gig economy’ work,⁸² they also become central mechanisms for accessing small amounts of short-term cash in return for work, and a prerequisite for accessing short-term labour through SMS, messaging platforms or platforms for organising labour. This means that a smartphone becomes

increasingly necessary for accessing retail and service jobs.^{83 84}
◦ *remittances and interpersonal money transfers, especially with the rise of micro-payments, including features such as WhatsApp Pay currently being trialled.*
◦ *forms of online or mobile-based payments, which have been extremely popular in Global South countries and are now starting to become more common in the Global North.*

2. Digital Identity
The myth of “one person, one device”

It has been said that identity is increasingly not ‘what you say you are’ but ‘what a particular service provider says you are’.⁸⁵ As individuals interact with the world and their devices, the data they provide is measured by their smartphone, organisations and service providers. A user’s digital identity is complex and multi-faceted. We are many things to many people and our identity changes depending on the context – mother, friend, worker, citizen – and our identity is necessarily flexible and diverse. For the purposes of this exploration, however, identity is understood as a digitised curation of the individual; one derived through their device, and through the data they generate, and which is then processed to define a narrative within social, corporate and government agencies.

Some elements which feed into digital identities for the purposes of this study are:

- *Device or platform level accounts (such as Apple ID, Google, etc)*⁸⁶
- *Location databases and place histories*
- *The contents of an individual’s smartphone*⁸⁷
- *Social media accounts (and data collected through off-site activities, such as information collected through the Facebook Login service)*⁸⁸
- *Digital health records*
- *Digitised government services*

- *Advertising profiles developed through online or real-world tracking, such as browser histories, spending habits and cookies*
- *Electronic or biometric passports and travel histories*
- *Behavioural habits*

Portable computing, the decreasing cost of sensors and devices and entrenched digitised systems have meant that many forms of identity are maintained via liquid surveillance, where constant access to measurements leads to detailed, increasingly complex representations of a person.⁸⁹

In examining digital identity, two perspectives emerge:

- *Identity and the individual – how individuals are represented via identity, and how this constructed identity is used to authenticate individuals by corporations, institutions and the state.*
- *Groups and relationships – how an individual’s identity interacts at the interpersonal level (e.g. parent-child, spousal, inter-community) or the more formal level (e.g. the state, corporations or NGOs).*

The Individual
The fractured digital self

An individual has many digital identities and their appropriate representation, interpretation and use are all crucial. Frequently, the factors that make up a digital identity in the form of a profile fail the individuals they are meant to represent. A digital identity can be connected to a verifiable asset that proves you are who you say you are, such as a passport or drivers license, it can be linked to an account, such as a username or device address, or it can be formed of many different data points, such as where you often go or how you use your phone, each describing element of an individual that is then compiled to make up a digital profile. These different approaches to digital identity are often thought of as separate, but increasingly technology innovation

in the digital identity space is blurring the boundaries. This can be most clearly seen in innovation in the fraud detection industry that increasingly combines all of the different elements of digital identities described above and adds to them lesser known techniques. This technology is referred to as ‘passive biometrics’ and includes elements such as how you normally hold your phone or type⁹⁰.

Identities that are rich with personal data, contain extensive interpersonal interactions or biometric data, are considered highly secure, or are owned by an authority are considered as verifiable and trustworthy. Digital identities that are used to validate an individual’s identity in contexts where proof of identity is crucial are often highly secure, rich with personal data, contain extensive biometric data and are usually owned by an authority are considered as verifiable and trustworthy.

Even the basic identifiers of what we tend to associate with identity, such as names, can be problematic.⁹¹⁹² A lack of cultural consideration may prevent users from passing computer-enforced data integrity checks^{93 94} or may punish them by falsely flagging them as inauthentic or fraudulent.⁹⁵ Such checks, for example, may not recognise ‘social names’ or linguistic variations, which may be common in some communities. Enforced real name policies lead to avoidable trauma (e.g. ‘dead-naming’ transgendered or transitioning individuals⁹⁶) and put at-risk individuals who need to compartmentalise and secure their online lives in precarious situations (e.g. pseudonymous activists or public figures and sex workers⁹⁷). Because of issues like these, individuals from minority or precarious communities often struggle to establish these forms of online representation.⁹⁸

Whilst most citizens think of this type of proof of identity as a given, such as a driving license, a passport or a residency card, that is not always the case. There are currently an estimated 1.1 billion people living without a verifiable ID,⁹⁹ and this is an area where smartphones are increasingly being considered as solutions by dedicated technology providers,¹⁰⁰ along with a wide range of other technologies including biometric data. In cases where a proof of identity document is lost or destroyed – for example, the sudden migration of refugees in the digital age – these new forms of more flexible identity can be ground-breaking. Biometrics and security in particular offer new methods to authenticate and administer aid to displaced populations.

An increasing amount of innovation can be found in this space, with UNHCR endorsing the increased use of biometrics for identifying and tracking refugees. This can be extremely valuable in providing essential services, such as reuniting families, but there are also increasing concerns about the disproportionate use of digital IDs. For example, the use of digital ID to access basic services such as access to food.

The Building Blocks system operated by the World Food Programme in Jordan is considered a successful trial of secure food distribution,¹⁰¹ minimising fraud through authenticating identity. Yet the privacy implications are enormous. Refugees in a state of dis-empowerment have little choice but to consent to the formation of these identities, giving up ownership of their fingerprints, irises and faces in exchange for basic necessities. The added permanence of these states through technology and policy lead to the further consolidation of power, as secure implementations of trust tend towards authoritarian politics.¹⁰² When travelling, individuals are subjected to biometric screening, contributing to growing repositories of at-the-border databases with little ability to consent. Travelling individuals – whether displaced or not – also risk the search of their electronic devices at borders, allowing authorities unprecedented access to the entire lives of people entering a nation. Often travellers have little understanding of their rights, or face diminished rights and threats for non-compliance.¹⁰³

Similar issues with biometrics occur in vulnerable US populations with increasing frequency. In September 2018, a US-based health insurer made global headlines by discontinuing traditional life insurance policies, offering plans only to individuals who agree to hand over their personal fitness data.¹⁰⁴ This offers benefits to those who can afford such devices and ignores the cyclical problems of poverty, nutrition and wellbeing,¹⁰⁵ whilst actively excluding those affected by poor healthcare and requiring daily surveillance from those who remain eligible. One month later, news of CPAP breathing machines carrying out surveillance of their user for insurance providers made headlines after a patient was denied a new breathing machine for not utilising their current device in line with provider expectations¹⁰⁶. The current wide-scale use of mobile phones for tracking and tracing Covid-19 cases has also shown the way in which identity and mobility tracking can be used for documentation and enforcement. This has led to a sudden rise in visibility of bio-surveillance techniques and mobility and behavioural tracking some of which

has revealed previously undocumented patterns across communities. Mass tracking and analysis of mobile phone data under lockdown has shown who can afford to stay at home and who cannot. In the US, mobile phone data showed the necessity of low-income communities to continue to commute, travel and move around in order to be able to work.¹⁰⁷

Emerging biometric technologies have come under increasing public and governmental scrutiny, with San Francisco passing the first ban of facial recognition in May 2019.¹⁰⁸ This was followed by Sommerville, Massachusetts, in June,¹⁰⁹ and Oakland, California, less than a month later.¹¹⁰ While these ordinances have only covered the acquisition and use by the city, much of the surrounding discussion covers the uncertainty of upholding such bans – particularly since much of the infrastructure is in place, whether controlled by government or private actors.¹¹¹ These debates are key to understanding the current and potential impact of biometrics-related design choices.

External to the device, the validity and reliability of an identity is crucial. Leveraging an identity to obtain the trust of others is a common trick for fraudsters, stalkers and law enforcement. This involves generating a crude identity for the purpose of impersonating someone online. Catfishing¹¹² is often used by law enforcement to surveil the online profiles of entire vulnerable communities, sometimes so brazenly that the practice is an open secret within the targeted community.¹¹³

Moving beyond the question of identity as a form of verifying who an individual literally is, there is also the question of identity as formed through digital profiles:¹¹⁴ That is, profiles and digital identities ascribed to individuals through daily habits, behaviours and actions. This can be data on where you frequently go, what time you come home, what apps you use, what you buy online and even what music you listen to. Each of these form data points that can be used to create profiles. Sometimes they are interpreted to paint a picture of who we are, from a type to a detailed overview of our preferences, tastes and tendencies. In this sense, identity is often a highly curated connection (whether the user is aware of this or not) between the individual, the device, platforms and communities.

“Mass tracking and analysis of mobile phone data under lockdown has shown who can afford to stay at home and who cannot”

From interests and hobbies, to socio-economic status and psycho-graphic profiles,¹¹⁵ the data brokering industry is built on the process of creating permutations of the individual, slices of many different digital selves – whether the individuals themselves ever see this profile or not.¹¹⁶ These data profiles are interpretations of the individual, yet for the external world they become directly attached to that individual’s identity and often lead to real world consequences, from scoring systems¹¹⁷ to filter bubbles to the cost of insurance plans and access to employment or housing.¹¹⁸ Very often this links to behavioural data tracking, in her book Surveillance Capitalism Shoshana Zuboff refers to this as ‘data that is about you but not for you’¹¹⁹.

Identity, Groups and Relationships
How identity is used by others

The presentation of self in the digital context is a cornerstone of how we present and interact socially with our communities.¹²⁰

Smartphones in particular stand out with regard to identity and group relationships. In many cases they are:

- *Assigned identities as in a one-to-one relationship, facilitated by existing design choices*
- *Used in many facets of an individual’s life, especially in safety, organisation and generating income*
- *Often relied upon by individuals to the point of precariousness,¹²¹ containing large amounts of data whilst being fragile and easily lost*

However, devices are often shared amongst family members in both coercive and voluntary contexts. Despite this, smartphones essentially remain ‘personal devices’ that are optimised for the singular user.

From observing usage patterns amongst different communities identified in this study, it is clear that how individuals operate in collaboration with others, on behalf of others and how devices are shared requires a fundamental remapping. For those living with disabilities, the elderly or in situations of care, primary users may be operating on behalf of others. Furthermore, as remote care through smart devices becomes a growing trend, the carer may not even be physically in the same

location. Equally, with smartphones at a premium in some temporary communities, such as migrant communities, they become a commodity where access is traded and facilitated through brokers to large groups of temporary users. This complexity associated with who a user actually is, and therefore what contributes to identity associated with a device, is not only difficult to navigate but also has practical implications for permissions, access, authentication and storage of data. The fluidity of a single device in these contexts has repercussions for device ‘ownership’ and goes against ‘smart’ or learning-based models for service delivery based on the principle of optimisation for a single owner of a device.

The data layer that sits beyond the device is also impacted by surrounding groups and individuals, with profiles being built and scores being generated by association with others. For example, the General Data Protection Regulation (GDPR) requires the disclosure of data collection, and requires that the data collection and related decision-making processes be justifiable and transparent, that subjects can request a copy of said data, and that it must be deleted if the subject of collection withdraws consent.¹²² Others go further to acknowledge the impact of inferred or associated data: how data on others – friends, relatives, colleagues or even members of the same group, club or neighbourhood – shape and influence an individual’s data profile or associated scoring. This advanced state of data processing and the interconnected data profiles it creates has led to philosophical and legal arguments that “one is dependent on other individuals as well as on the things surrounding them [...] In fact, we are living a true identity revolution.”¹²³

3. Agency
Inherent vulnerabilities in dependency

Device ownership unlocks agency for people in their daily lives – acting as both an ‘enabler and a magnifier’ – and this means that smartphone use can bring both freedom and control.

The structured nature of smartphones, connectivity and data storage determines how users interact and operate in a connected society and the opportunities and protections afforded to them. These dynamics interact with socio-political constructs that impact an individual’s agency. In this sense, agency as it applies to this review has two interconnected elements: the choice of how a device is configured, and how the device and its data are utilised either by the individual, or against them by an adversary or authority.

Power relations
Amplifying real-world structures

Every instance when an individual’s digital life intersects with another individual or organisation is a negotiated power exchange. The components of digital participation are subject to social dynamics, control, abuse and agency of relationships among individuals, their communities and state, corporate and other institutions. In vulnerable populations, power relations are often deeply unbalanced and detrimental. This reality is often reflected as new technologies are adapted and utilised and as individuals, organisations and institutions utilise these tools to extend and amplify existing power dynamics.

Examples of how power dynamics play out through smart devices can be found by looking at the intersection of economic freedom and connectivity. In lower-income households, financial constraints can keep individuals in inappropriate living situations, sharing housing with people they may consider to be unsafe or untrustworthy. As saving money is a priority, the need for connectivity, such as mobile phone service, and the restrictive nature of contracts encourages people to share plans with untrusted individuals. One study describes “[people] trapped in plans with estranged partners, distant family members, and others they didn’t know well, such as temporary roommates, or people they’d lost touch with.”¹²⁴ Low-cost price plans, cheaper services, discount vouchers and minutes for data all target low-income communities at the expense of contract lock-in and privacy.

The interplay of economics and poverty extends further, into the over-surveillance of minorities and vulnerable communities through policing their finances.¹²⁵ Often, the collection and analysis of financial behaviour is used to draw negative conclusions about a community for the purpose of policing or limiting financial choice. For example, Paul LePage, the governor of Maine, released data to the public detailing over 3,000 transactions from welfare recipients and was successfully elected on a campaign that highlighted the number of times “public money” had been used in strip clubs, liquor stores or bars. At his campaign’s core was a push to limit access to state benefits.”¹²⁶ As mobile phones become increasingly central to payment systems, these questions will become more relevant and more poignant for low-income communities, refugees and others living with a range of

digital financial surveillance measures empowered by an environment driven by credit checks, welfare fraud and tax evasion detection. The pressure to move towards digital money in the context of public health concerns, in particular a move away from cash and credit cards due to the spread of viruses, will accelerate this trend in the coming years for all communities.¹²⁷

In Australia, welfare cards that restrict purchases to government-approved products are in active trials in vulnerable, remote indigenous communities.¹²⁸¹²⁹ These technologies increasingly “decide who gets public services, who is denied public services, and how we monitor and police the most marginalized people in our society.”¹³⁰ Alongside the cashless welfare card, the Australian government has deployed a “Robodebt” programme, combining information from welfare infrastructure with often incomplete data from employers.¹³¹¹³² This process is almost entirely automated and routinely produces erroneous judgements. The Robodebt programme is linked with several suicides from vulnerable targets of automated debt collection.¹³³¹³⁴¹³⁵ Combined with issues of identity – particularly health and health care – corporate and government surveillance of poor communities is punitive, overreaching and often intended to make public services more economically efficient.¹³⁶ In November 2019, two class action lawsuits against the legality of Robodebt were permitted to proceed by Australia’s High Court, despite late stage intervention by the incumbent coalition government. A member of the Federal Opposition described the government’s response as “a very late admission there is something rotten at the core of Robodebt”.¹³⁷

Examples of welfare cards and other enforceable digital payment systems are also prevalent in precarious communities across the Global South. The Red Cross is trialing blockchain-backed credit or payment systems as a form of economic stimulus in Kenya,¹³⁸ with plans to expand the program into Cameroon, Malawi, Myanmar, Papua New Guinea and Zimbabwe if initial trials are successful.¹³⁹ These services are described as forms of individual and community empowerment, but as Blockchain transactions in general are not private unless this feature is specifically designed into the system, this creates an unprecedented level of control and transaction surveillance for those who administrate the payment network in economically precarious societies.

Within the device, agency is also not guaranteed: for example, external interference and surveillance by authorities can interrupt the social trust of connected communities.¹⁴⁰ In the UK, for example, schools and universities are specifically instructed to monitor the communications of students and are required to report instances of suspected radicalisation.¹⁴¹ Migrants, asylum seekers and those in poverty are also exposed through tech dependency and surveillance which tends to centre on ‘young men’ – terrorism and counter-terrorism, gangs and crime. This includes surveillance of devices, but also activity, browsing history and social associations on platforms such as Instagram, Facebook and SoundCloud. This activity is designed to infer gang hierarchies or potential radicalisation.

Surveillance techniques are not only deployed by institutions but are also prevalent among violent partners or caregivers. There have been public cases of companies offering easy-to-use surveillance tools that weaponise various aspects of an individual’s status, such as their whereabouts, images or metadata.¹⁴² Verifiable but anonymous, pseudonymous or highly controlled identities can provide everyday protection to particularly vulnerable populations.

Power relations can in some cases expose a community. For example, Tactical Tech’s previous work with sex workers¹⁴³ showed that smartphones were not only a valuable device for sex workers for access to work, resources and safety, but were also frequently confiscated by the police or controlled by procurers, pimps and traffickers. For this reason the concept of the mobile phone as a ‘personal’ device was complicated. Sex workers, for example, create compartmentalised pseudo-identities to protect themselves from their clients whilst making a living,¹⁴⁴ operating in a paradoxical state of notoriety and anonymity.

In residential areas, power structures are amplified through smartphone apps that encourage citizen surveillance of their neighbours (Nextdoor) or their community (Citizen). Both apps allow users to report suspicious activity, post photos and discuss events in detail, often with problematic outcomes. For years, Nextdoor has struggled with widely-reported examples of racism on its platform.¹⁴⁵ When Citizen first debuted as Vigilante in 2016, the resultant outcry compelled Apple to remove it from the App Store.¹⁴⁶ The re-branded app launched shortly after, and in 2017, Citizen raised a US\$12m round of funding based on its user growth.¹⁴⁷

In reverse, however, we are witnessing the (re)rise of cellphones as ‘sousveillance’ device – a term coined to refer to bottom-up surveillance and documentation of abuses of power by individuals and institutions, brought about by the early rise of the mobile phone camera and video. Non-profits such as Witness have worked extensively to empower individuals to utilise smart personal devices for documentation. In collaboration with other organisations, such as The Guardian Project, they have not only enabled individuals to utilise such technologies for ‘sousveillance’, but also put in place checks and balances that enable such documentation to take place safely and effectively. This includes guides and advice¹⁴⁸ but also tools that build in mechanisms that increase safety for individuals, such as Obscuracam¹⁴⁹.

Beyond smart apps, companies like Amazon Ring and Nest use home security (especially smart-camera enabled doorbells) to create residential barriers and otherness, treating outsiders as a potential threat. In November 2019, it was revealed that Amazon planned Ring-powered “Watch Lists” biometrically comparing live video from their network of smart door security to alert homeowners to “suspicious” individuals outside their homes.¹⁵⁰ Ring already partners with 400 police forces across the United States,¹⁵¹ further amplifying real-world power structures and the potential targeting of precarious groups.

Internet-connected devices in the home have presented new mechanisms through which to exercise power relations. Emerging research illustrates how smart devices – from speakers and light-bulbs to cars and home appliances – are used in domestic contexts to suppress agency. Interviews with abuse victims, lawyers, shelter workers and emergency responders detail how smart home technology is used to abuse women. Abusers — using apps on their smartphones, which are connected to internet-enabled devices — remotely control everyday objects in the home, sometimes to watch and listen, other times to psychologically harass women.¹⁵² This behaviour is similar to the surveillance of women through their devices, but is more structural and less visible, allowing an abuser in many cases to remove or control physical agency through direct manipulation of a connected environment.

Control

Trade-offs between automation, simplification and choice

No matter how much an individual relies on their smartphone, the struggle to control the device remains and often manifests itself in the difficulty in understanding what choices they can make and why and how things are happening on their phone. Some features and settings may be needed by the user – for example optimising battery life or controlling data usage – that may even already exist on a mobile operating system, but a large number of users do not understand how to access or use them effectively. This puts into focus a set of problems related to smartphones and a set of trade-offs that needs to be navigated. Systems that optimise functions and simplify processes can create greater efficiency and enable smoother, more seamless experiences for the user, and in some cases even provide adaptive and smart configurations to optimise based on a user’s bespoke needs. Within this lies a contradiction. Despite the challenges of exposing device settings to users and their ability to understand how to control their devices, the opposite approach – simplified, and often automated, systems reduce transparency – can equally be frustrating and confusing for the user as they can remove the ability of users to exercise control and choice.

In some systems, seamless automation and optimisation advances ‘under the hood’ of the platform, service, app, device or operating system, which could be significantly beneficial to many users. For example, the UC Internet Browser (developed by the Chinese mobile Internet company owned by Alibaba, and currently the third most popular web browser on mobile devices [along with Chrome and Safari])¹⁵³ is improving the speed and cost of data transfer by using compression, the cloud system and smart download management. This creates efficiency, enhances the speed of data and limits costs. However, it also increases security and privacy concerns. The same features can be found in Facebook’s Onavo VPN. In this case, a service that provided speed, compression and the ability for users to monitor and track their data usage on metered connections was ultimately taken off the market after it was revealed that all device behaviour was tracked and stored by Facebook, arguably without the full consent of the user.¹⁵⁴ Opera, a company that provides a free web browser for mobile devices, also offers a free VPN service designed to increase performance and lower data usage on metered connections. It has received similar scrutiny.¹⁵⁵

“Two somewhat contradictory trends are currently at play in technology design: seamless automation and enhanced user control. These represent two different approaches to interaction design; either removing choice and complexity from the user in order to enable an optimised and simplified experience or providing granular levels of control directly to the user.”

In other systems, dashboard-like levels of enhanced user control are increasingly being deployed. This is especially the case with approaches to personal data management as well as security and privacy settings. There are problems, however, with how such systems are designed and implemented. They can be simply too much for a user who doesn’t necessarily always understand the implications of their choice, or they may simply never be explored.¹⁵⁶ After the change in European regulations with the GDPR, some efforts were made to improve such interfaces. Yet one survey confirms that “although most of the users are aware of the privacy settings, most of them do not change their privacy settings from default settings”¹⁵⁷ and “less than 5% of the users we surveyed had changed any settings at all. More than 95% had kept the settings in the exact configuration that the program installed in.”¹⁵⁸ Some research suggests that the reason that such flexibility does not necessarily expand the ability of the users is not necessarily because users don’t want to adapt and change their devices, but largely because of how these options are presented. For this reason, different approaches may be necessary, for example dividing types of users into clear and descriptive categories and creating a layer on the top of granular settings that would make it easier to understand the choices.¹⁵⁹

Two somewhat contradictory trends are currently at play in technology design: seamless automation and enhanced user control. These represent two different approaches to interaction design; either removing choice and complexity from the user in order to enable an optimised and simplified experience or providing granular levels of control directly to the user. Both have their advantages and disadvantages for people living in precarious situations. More work needs to be done in this area to better understand the trade-offs. In addition, ‘privacy-by-design’¹⁶⁰ and ‘security-by-design’ principles could be further explored, with more core principles factored in to the initial build of the system.

4. Multipliers

Two final cross-cutting themes that came out of the literature review can be thought of as multipliers, or factors that lie on top of the other issues and need to be considered in designing for these communities:

1) the impact and influence of time and

2) the challenge of designing not just for individual users, but millions of individual users.

Scale, place and time

Key factors in designing for precarious living

The shifting, temporary and fragile nature of the situations in which the priority communities of this landscaping study find themselves means that time is an important factor in designing systems. This applies to everything from the device as lifeline to the questions related to permissions, access and control. Situations can change suddenly and unexpectedly. For example, a natural disaster, such as a forest fire, may plunge a user from continuous access to a stable smartphone into a situation of extreme vulnerability in a matter of moments. Increasingly, Australia’s 2019-2020 summer climate-amplified wildfires has seen a massive increased dependency on smartphones fuelled by the introduction of new, highly sensitive fire-mapping apps for iOS and Android. However, as smartphone infrastructure failed suddenly across large regions in affected areas, users quickly needed to fall back to ‘older’ technologies (AM radio, etc). The full implications of this are yet to be explored.

Equally, a mugging or a sudden case of domestic violence may instantly change a user’s relationship with their smart phone, but the pressures and psychological impact of these different scenarios may vary considerably. For those living in poverty or for refugees, situations may change unexpectedly and irreversibly: for example, access may be intermittent, or temporary constellations of users may emerge and change frequently.¹⁶¹

Because of the transient nature of circumstances, decisions made about key factors such as consent, access, permissions and even identity may change over time – sometimes gradually, sometimes suddenly. Currently, transience is so poorly implemented into designed

systems that even privileged economic migrants face friction such as their smartphone accounts being tied to the region they departed, unable to be re-set to their new country of residence.¹⁶² This friction multiplies with precarity and solutions need to be thought of with a certain flexibility and plasticity in mind. This can be particularly difficult for users to navigate especially when user habits are well formed¹⁶³ or when the situation involves stress and trauma or there is a lack of choice. Studies on the efficacy of digital security training, for example, have proven that users who are under stress are less able to absorb new technical skills and change well-worn habits.¹⁶⁴

The design of smartphones and the web of data collection that it facilitates through the many apps and services that it delivers does not take into account how things shift over time. This is not only the case for extreme examples, as highlighted above, but also for more everyday occurrences. From moving home to becoming unemployed, default settings and data-driven profiles do not afford for the idea of change and this can create frustrating barriers to technology use for some whilst retraumatising others. There are many examples of individuals who have suffered cancelled weddings, lost pregnancies, deaths in the family and so on, where advertising profiling, default settings or seemingly useful bonus features, such as ‘your year in review’ can have devastating effects.¹⁶⁵ Micro-profiling may have many benefits but it is not designed with changes in circumstance in mind. However, this is not to make the case for more accurate profiling where algorithmic acknowledgement of these changes may be even worse for most privacy advocates, but rather to question in the first place the logic on which such detailed profiling is built.

We need principles not for a few individuals but for millions

This study focuses on the user as the individual. However, what increasingly matters is the aggregate and how the use of digital and data-driven personal technologies, such as smartphones, by millions of individuals impacts cultural and social norms and transforms dynamics between groups, institutions and societies at large.

“the desire for simplification of designed systems and interfaces, and this lack of flexibility is at odds with an increasingly precarious and changing global world.”

Different approaches to design are needed when we encounter the question of how to make technologies for individuals at scale. In the case of disaster, the fact that large numbers of individuals have smartphones creates new opportunities for utilising and developing technologies and also brings new challenges. Some examples include initiatives that:

- *explore mobile crowd-sensing,¹⁶⁶ such as apps to operationalise mass networks of sensors within individual mobile phones as a way of producing early warning systems for earthquakes*
- *can use recorded mass changes in normal device use behaviour as triggers that may indicate that a disaster or crisis is occurring*
- *use mobile devices to solve (small) group problems in times of crisis, such as public way-finding¹⁶⁷ and crowd control*
- *seek to activate sensors within smart cities for disaster detection, control and response in urban areas, or can be placed in semi-rural areas as powerful prevention and mitigation systems, such as for landslides, tsunamis, earthquakes, floods and forest fires¹⁶⁸*
- *track and analyse mass movements of migrants and displaced persons within and across borders, but this is accompanied by a host of ethical issues¹⁶⁹*
- *utilise the power of networks and platforms, including ‘social media listening’ but also new features introduced by Facebook, such as Safety Check, a system which attempts to use social graphs to let large networks of friends know that people are safe in times of crisis (a system that has received a high degree of criticism)¹⁷⁰*
- *exploit the ubiquity of mobile phones for tracing and tracking human behaviours, mobility and contact with others at scale, as in the case of Covid-19.*

Many of these systems could be highly effective but at the same time increase mass surveillance mechanisms. This leads to a hidden danger within techno-solutionism,¹⁷¹ which is that a kind value tension or ‘issue blindness’ can emerge.¹⁷² Whilst working to fix one set of problems, for example natural disaster monitoring through nationally enabled smart device sensors, another set of problems related to fundamental freedoms and civil liberties arise. Society, industry and the institutions that regulate and control them are only at the beginning of this journey.

Now that the infrastructure is in place, in almost every pocket, home, town and city in the world, and its use is being normalised for everything from interpersonal transactions to payments, the impetus to use it in every way possible is increasing. However, the critical thinking, public debate and regulatory frameworks necessary to assess its edges are not in place; nor are the design principles and frameworks that will lead us forward into designing tools that truly meet our needs whilst respecting societal values, rights and freedoms. Nowhere are the challenges of this more evident than in the context of designing the Smart City, a kind of container and melting pot for bringing together all the issues we have highlighted in our research. The 2020 shelving of Alphabet’s SideWalk Labs \$2bn Toronto project will no doubt serve as a valuable future case study about just how complex such aspirations are.

There are clear challenges ahead and a large amount of work is still needed to bring such thinking into mainstream design practices. Design assumptions about identity are mainly driven by the desire to facilitate authentication, device or service operation and at times self-expression but overlook the multi-faceted ways that identity works bureaucratically, culturally and for different communities. Universal design deployed across varied communities results in incomplete or ill-considered implementations of identity. Anticipated use cases for platforms and devices can severely restrict user agency, and additional dependency, this amplifies the failings of the design. Finally, the rigidity of these solutions are the result of context collapse: the desire for simplification of designed systems and interfaces, and this lack of flexibility is at odds with an increasingly precarious and changing global world.



Part III: Reflections and Where to Start

Technology amplifies existing structural issues rather than creating new problems. This stands in stark contrast to popular discourse, in particular in the media, which tends to infer that smartphone and related technologies generate new political and social issues. At Tactical Tech, however, we take the position that they instead extend and amplify political and cultural tensions and pre-existing dynamics in society. This important distinction is an essential starting point in changing the technology design process.

If we first accept that the design, usage and widespread implementation of digital technologies will mirror biases, political ideologies and shifting dynamics and tensions in society, then it becomes much easier to imagine what their unintended uses, blindspots and trade-offs may be. Such an approach, of ‘technology as mirror’, can then more easily be factored in to the design process. This shift needs to take place not only at the design level, but also should be a central element in decision making about engineering choices – such as machine learning design, policies and practices developed around service delivery and control, and the responsibility of companies to anticipate what may go wrong. This may not be a central factor in the business model of most technology companies which are often quick to market and favour ‘testing in the wild’. However, consistent crises and scandals in the tech industry over the past five years, such as the UK teenager Molly Russell whose exposure to self-harm through Instagram was linked to her suicide¹⁷³, have shown that the cost of ignoring these problems-waiting-to-happen also hurts the health of tech businesses, changes the regulatory environment and ultimately impacts their bottom line. In short, ignoring the social, political and cultural dynamics of large-scale technology roll-out is at best bad for business and at worst negligent and irresponsible business practice that can lead to fines, lawsuits and the intervention of the State.

A shift in understanding of ‘technology as mirror’ would not only lead us to seek better and more robust models for technology design but also encourage companies at every level, from feature designers to executives and VPs, to think ahead and take responsibility for what may happen to the technologies they are designing and promoting as they scale and become fully integrated into society.

“Technology amplifies existing structural issues rather than creating new problems”

As technology designers and engineers become the architects of the new built environment, more needs to be done to ensure they have the skills, knowledge and tools they need to make the right decisions. This not only means widening their toolkit and having the support of leadership but also ensuring they have a rigorous educational grounding in ethics and work in diverse teams. Many of the tools designers and engineers are making are extremely complex. For this reason, more needs to be done to ensure that design teams have access to in-house and external specialists who understand the intersection of technology and politics and the implications of working with an understanding of rights, justice and sustainability frameworks.

As existing solutions are improved and extended and new projects are developed, there needs to be substantive engagement with communities and subject experts with an eye toward collaboration. Current approaches to designing for communities often consist of two main methods:

- *classic user-led design research, largely through interviews and observation, and*
- *direct collaboration with non-profits to provide access to and adaptations of products that answer a distinct set of needs.*

These have both proven to be effective methods in some circumstances, but they also have significant shortcomings. Working directly with specific communities to find solutions can lead to symptom-related fixes, and needs to be done in collaboration with existing actors and sectoral experts, who are often overlooked. In each of the sectors reviewed in this study, however, there are experts, researchers and companies working in-depth on technological solutions for each scenario. In order to go further in addressing the needs of a more diverse set of users, complementary methods, such as designing for difference, for consequences (designing from the future back) and understanding trade-offs and unforeseen effects, should be introduced. This would extend the learning process, allow for stress testing of ideas and potentially lead to new features and innovation for all. Solutions that seek to resolve challenges for people living under extremely challenging conditions could also be useful to a broader group of users, especially those who rely on phones for other kinds of relationships where dependency is a key factor.

For example, the same energy efficiency solution needed by someone in a crisis could also be valuable to a parent trying to reach their child whose battery is almost depleted.

Design methods:

There is an increasing body of theoretical work, research and efforts at awareness-raising that advocate for an ethical approach to technology design. Often, these efforts champion the needs of a diverse group of users outside of a ‘typical’ user group and seek to anticipate the life cycle of a product once it leaves the design studio and is used in the real world.¹⁷⁴

Concepts such as ‘affordance’ in interaction design can help to enforce a more nuanced understanding of technology design. Affordance as a concept in design terms recognises that “users’ social context, abilities, and purposes define their interactions with technologies.” and therefore have to be factored in when designing objects and systems and understanding that these factors will impact how a user reacts, behaves or is able to utilise an intended design.¹⁷⁵ Such research can be helpful in understanding users not as generic (even within ‘user types’) but as highly influenced by their context and their lived realities, as well as their prior experiences of using technology. By extension, the same is true of the designers themselves. This way of thinking reflects a broader shift in the field of technology design, which has led to calls for greater diversity in technology design teams.¹⁷⁶ Having more varied design teams with different lived experiences may by its very nature lead to shifts in processes or product outcomes, or perhaps even in the identification of the core problems that need to be solved.

Numerous existing methodologies seek to aid a more holistic approach to technology design, including:

- *Participatory design*^{177 178}
- *‘Do-no-harm’ principles, as rooted in conflict resolution and humanitarian work, increasingly applied to health, robotics, AI and digital security*¹⁷⁹
- *Value Sensitive Design, of which there are 14 different methods*¹⁸⁰ *including tools such as ‘Envisioning Cards’*¹⁸¹
- *The Iceberg Model, which was designed to aid systems thinking*¹⁸²
- *Various toolkits created by design studios, such as: Artefact Group’s ‘The Tarot Cards of Tech’*¹⁸³, *and IDEO’s ‘Designer’s Toolkit for Tackling Tough Problems’*¹⁸⁴

There are many more design methods that need further exploration and space for testing in the technology design space, such as consequential design, which uses an ‘if this, then what?’ approach to design.¹⁸⁵ Some of these design thinking tools can prove extremely useful when helping design and product teams plan more responsibly and factor in new questions to the design and development process. Tactical Tech has extensively used the Tarot Cards of Tech by the Artefact Group in its workshops with design students, practitioners and product leads at technology companies and found that they are an extremely useful tool for getting teams to think beyond existing design thinking and outside of the (commercial) box. More needs to be done to teach and develop design thinking tools that challenge dominant methods of user and human-centric design. Much has been done already in the design of physical and consumer goods to rethink the design process and the role of responsibility and sustainability, for example by the Ellen MacArthur Foundation and their extensive educational work on circular design.¹⁸⁶ A similar shift in consciousness is needed in the technology design space.

The policy sphere – from regulators to think tanks to policy makers in technology companies – increasingly acknowledges the need to consider design and

engineering decisions and their possible ramifications. This tends to focus on issues of responsibility and accountability¹⁸⁷ and be framed as a duty of care of the design process.¹⁸⁸ However, the gap between regulation, policy and product is closing – even within technology companies. A recent public document by Google’s policy team advocates the need for regulators of the technology industry to “...encourage the design of products to avoid harm to individuals and communities,”¹⁸⁹ recommending that designs not only need to “account for and mitigate” potential harms, but also need to “... [take] particular care with sensitive information that can pose a significant risk.” This indicates that in the design process, there is also a need to zoom out from the core functions of the device, thinking not only about the interactions and the experience, but also about the additional data layer that is generated by the use of the smartphone, and increasingly about the policy and regulatory environment. This is particularly evident in the case of the Age Appropriate Design Code¹⁹⁰ that was compiled in the UK under the leadership of the Information Commissioners Office and compels technology companies to solve a wide range of policy problems at the design level.

Next Steps

As previously stated, this research overview and summary is just the start of a process. It takes a sweeping look at different issues in an attempt to bring them together and to understand more about their common themes. The intention is to start new conversations about how to work across sectors, disciplines and issues areas, to reflect more deeply on the use of technology by different communities, their needs and the challenges and opportunities of using personal technologies within difficult, unpredictable and challenging environments. This study is also a plea to recognise design as not only problem-solving but also as problem-making, and further evidence that the technology design tools and methods that are predominantly utilised are not always fit for purpose. Factoring in diversity and ethics to the design and development process is not a gesture, but rather an integral part of good product design. If we will increasingly rely on personal technologies in the future, not only to navigate daily life but also to organise society, we will need to find ways to design in the public interest using models that recognise the shortcomings of consumer-led, individualistic design and instead design for ‘society as user’.

¹ <https://onlineacademiccommunity.uvic.ca/globalsouthpolitics/2018/08/08/global-south-what-does-it-mean-and-why-use-the-term/>

² Global mobile consumer trends, 2nd edition, Deloitte

³ Isabel Lorey, *State of Insecurity: Government of the Precarious*, (London: Verso) 2015

⁴ See, for example, Nic Fildes, ‘Mobile phones and AI vie to update early disaster warning systems: Networks of sensors can predict earthquakes with greater precision’, *Financial Times*, March 2019

⁵ Neil Ungerleider, ‘Why Your Phone Doesn’t Work During Disasters – And How To Fix It’, *Fast Company*, April 2013

⁶ US Internet Use in 2015, Pew Research Center, Internet and Technology

⁷ See initiatives like One Concern

⁸ See for example: Nokia Saving Lives Program working with Red Cross and Drones, the UNDP expert summer school relief and tech innovation (including Google employees as trainers).

⁹ Global Humanitarian Technology Response Conference, held in 2018 in Silicon Valley

¹⁰ Trevor Nace, ‘How Technology Is Advancing Emergency Response And Survival During Natural Disasters,’ *Forbes*, December 2017

¹¹ Tim Moynihan, ‘The New Tech of Disaster Response, from apps to aqua-drones’, *Wired*, 29 August 2015

¹² Laura Bliss, Could Self Driving Cars Speed Up Hurricane Evacuations?, *Citylab*, 12 October 2016

¹³ Ben Coxworth, Smart Harness could turn rescue dogs into four-legged reconnaissance systems, *New Atlas*, 5 May 2014

¹⁴ See for example: ‘A framework of community inspired distributed message dissemination and emergency alert response system over smartphones’, 2016.

¹⁵ The Best Apps For Tracking Fires and Smoke Pollution Near You, *Gizmodo Australia*, 10 December 2019

¹⁶ Why Waze Isn’t the Best Choice for Commuters During Early Stages of Wild Fires: Check Better Sources, *Auto Connected Car News*, 7 December 2017

¹⁷ European mobile operators share data for coronavirus fight, *Reuters*, 18 March 18 2020

¹⁸ Poland’s coronavirus app offers playbook for other governments, *Politico*, 4t March 2020.

¹⁹ Apps and Covid 19, *Privacy International Website*.

²⁰ UNHCR, *Figures at a glance*

²¹ <https://www.worldbank.org/en/news/press-release/2018/03/19/climate-change-could-force-over-140-million-to-migrate-within-countries-by-2050-world-bank-report>

²² Matthew Brunwasser, ‘21st Century Migrants Essential: Water, Shelter, Smartphone’, *New York Times*, 25 August 2015

²³ Koen Leurs and Kevin Smets, ‘Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe’, *Utrecht University*, January 2018

²⁴ UNHCR, ‘Connecting Refugees, How Internet and Mobile Connectivity can Improve Refugee Well-Being and Transform Humanitarian Action’, *Geneva*, September 2016

²⁵ Rianne Dekker¹, Godfried Engbersen, Jeanine Klaver, and Hanna Vonk, ‘Smart Refugees: How Syrian Asylum Migrants Use Social Media Information in Migration Decision-Making’ in *SI: Forced Migrants and Digital Connectivity*, 2018

²⁶ Sandra Ponzanesi, ‘Digital Strangers at Our Door: Moral Panic and the Refugee Crisis’, *Europe Now*, 2 July 2018

²⁷ See for example, James O’Malley, ‘Surprised that Syrian refugees have smartphones? Sorry to break this to you but you’re an idiot’, *The Independent*, 7 September 2015

²⁸ European Parliament, Directorate-General for Internal Policies, *Reception of Female Refugees and Asylum Seekers in the EU, Case Study Germany*, 2016

²⁹ UNHCR, *Connecting Refugees*

³⁰ See for example, Amy Weiss Mayer, ‘Apps for Refugees’, *The Atlantic*, 5 May 2017,

³¹ See Philip Oltermann, ‘Syrian Refugees design app for navigating German bureaucracy’, *The Guardian*, 5 August 2016

³² Techfugees Global Summit

³³ See for example, European Parliamentary Research Service, ‘Technological innovation for humanitarian aid and assistance, European Parliament, May 2019

³⁴ Mark Latonero and Paula Kift, ‘On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control’, *Data and Society Research Institute*, January 2018

³⁵ Marie Gillespie¹, Souad Osseiran, and Margie Cheesman, ‘Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances’, *The Open University*, March 2018

³⁶ Morgan Meaker, ‘Europe is using smartphone data as a weapon to deport refugees’, *Wired*, July 2018

³⁷ United Nations Human Rights Office of the High Commissioner, *Statement on Visit to the USA* <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22533&LangID=E>

³⁸ Joseph Rowntree Foundation, <https://www.jrf.org.uk/blog/we-have-new-way-measure-poverty-now-act-solve-it>

³⁹ *Income and Poverty in the United States: 2018*, United States Census Bureau.

⁴⁰ Stephen A. Rains and Eric Tsetsi, ‘Smartphone Internet access and use: Extending the digital divide and usage gap,’ in *Mobile Media and Communication*, 2017

⁴¹ <https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/>

⁴² *ibid.*

⁴³ See: Apple T2 Security Chip, *Security Overview*, Apple, October 2018, which describes the Secure Enclave.

⁴⁴ ARM TrustZone Technology overview

⁴⁵ Building Titan: Better security through a tiny chip, *Android Developers Blog*, 17 October 2018

⁴⁶ Remarks by subjects interviewed by Simply Secure, ‘Straight Talk: New Yorkers on Mobile Messaging and Implications for Privacy’, 2015.

⁴⁷ 2bn phones cannot use Google and Apple contact-tracing tech, *The Financial Times*, 20 April 2020.

⁴⁸ Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, (St. Martin’s Press) 2018

⁴⁹ See Zygmunt Bauman & David Lyon, *Liquid Surveillance: A Conversation*, (New York: Polity Press) 2010

⁵⁰ For example, RoarForGood.

⁵¹ See for example the partnership between IBM and Nokia

⁵² Sonia Livingstone, One in Three: Internet Governance and Children’s Rights, Unicef, January 2016

⁵³ Leurs and Smets, ‘Five Questions for Digital Migration Studies: Learning from Digital Connectivity and Forced Migration In(to) Europe’, 2018

⁵⁴ <https://www.jrf.org.uk/blog/we-have-new-way-measure-poverty-now-act-solve-it>

⁵⁵ Heather Davidson, ‘The Internet is Leaving Queers Behind’, Autostraddle, 7 August 2017

⁵⁶ Ben Collins, Twitter Trolls Are Reporting Pro-LGBT Muslim WOMen to Their Governments Where Punishment Can Mean Death, Daily Beast, 20 June 2016

⁵⁷ Young and unafraid: queer criminology’s unbound potential, Panfil, 2018

⁵⁸ Grant et al, ‘Injustice at Every Turn: A Report of the National Transgender Discrimination Survey’, 2011

⁵⁹ Melanie Stray, Online Hate Crime Report, Galop.org, 2017

⁶⁰ <https://www.pride.com/viral/2018/7/12/man-attacked-being-gay-goes-viral-after-posting-grinning-selfie>

⁶¹ See Tactical Tech’s research on Data and Dating

⁶² See Tactical Tech’s ‘Quantifying Homosexuality: A Critique, Our Data Our Selves, 2018

⁶³ Monitoring being pitched to fight Covid-19 was tested on refugees, Bureau for Investigative Journalism, 28th April 2020.

⁶⁴ See for example, ‘Which Mobile Phones Work Best for Disaster Responders and Humanitarian Aid Field Teams?’, ICT works, 5 March 2018,

⁶⁵ See for example, tips on how to extend battery life, for an example of work-arounds

⁶⁶ See for example, the GSMA’s Connected Society: The State of Mobile Internet Connectivity 2019 report, published July 2019

⁶⁷ Jessica Leber, ‘This New Kind Of Credit Score Is All Based On How You Use Your Cell Phone’, Fast Company, April 2016

⁶⁸ Official monthly data by Google, see for example: <https://fossbytes.com/most-popular-android-versions-always-updated/>

⁶⁹ See the Android Compatibility Program: <https://source.android.com/compatibility/overview>

⁷⁰ See for example, ‘Used Smartphone Industry on the Rise’, Forbes, December 2017,

⁷¹ See for example, low-cost tower that can collapse for transport in the luggage compartment of an airline. Set up takes seven minutes, custom parts can be 3D printed in the field, and the cost is about \$600 (US \$530)

⁷² See Ericsson Response project

⁷³ GSMA, Refugees and Connectivity

⁷⁴ See for example Tigo in El Salvador, a leading mobile phone operator providing zero rating, in Nic Fildes, ‘Mobile phones and AI vie to update early disaster warning systems’, Financial Times, 29 March 2018

⁷⁵ Amy L. Gonzales, ‘Health benefits and barriers to cell phone use in low-income urban U.S. neighborhoods: Indications of technology maintenance’, Indiana University, 2014

⁷⁶ Amy L. Gonzales, Linday Ems and Venkata Ratnadeep Suri, ‘Cell phone disconnection disrupts access to healthcare and health resources: A technology maintenance perspective’, Indiana University, 2016

⁷⁷ See for example, Reginald Dwayne Betts, How the Surveillance State Destroys the Lives of Poor Whites and People of Color, The American Prospect, 22 June 2018

⁷⁸ Tsetsi, ibid

⁷⁹ See for example, Farhad Manjoo, ‘For Millions of Immigrants a Common Language: WhatsApp’, New York Times, 21 December 2016

⁸⁰ Josh Constine, ‘WhatsApp Hits 1.5 billion monthly users. \$19B? Not so bad.’, TechCrunch, 31 January 2018

⁸¹ Tsetsi, ibid

⁸² 15.8% of American workers participated in gig labour in 2015, up by 5% over the previous year. See Kats and Krueger, ‘The Rise and Nature of Alternative Work Arrangements in the United States, 1995 - 2015’, 2016.

⁸³ See Richard Partington, ‘Number of zero-hours contracts in UK rose by 100,000 in 2017 – ONS’, The Guardian, 23 April 2018

⁸⁴ Noah Smith, ‘On Call Work Schedules Make it Hard to Have a Life’, BusinessWorld, 19 June 2018

⁸⁵ Megan Angelo, You Are What Google Says You Are, Portfolio.com, February 2009

⁸⁶ Google provides a breakdown of collected data that are used to build identity tied to Android and other company services

⁸⁷ The Apple support documentation for iCloud offers a concise summary of a device-based digital identity

⁸⁸ Facebook Login allows for the exchange of user data between Facebook and third party companies, often with user data/identity exchange between two or more entities:

⁸⁹ Bauman and Lyon, Liquid Surveillance

⁹⁰ See for example Mastercards NuDetect technology. <https://nudatasecurity.com/solutions/nudetect/>

⁹¹ Huang, G., & Li, K. (2016). The Effect of Anonymity on Conformity to Group Norms in Online Contexts: A Meta-Analysis. International Journal Of Communication, 10, 18. Retrieved from <https://ijoc.org/index.php/ijoc/article/view/4037>

⁹² Siegel, J., Dubrovsky, V., Kiesler, S. & McGuire, T.W. [1983] Group processes in computer-mediated communication. Organizational Behavior and Human Decision Processes, 37, 2. Retrieved from <https://www.sciencedirect.com/science/article/abs/pii/0749597886900506>

⁹³ James Bennett, ‘Let’s talk about usernames’, b-list.org, 2018

⁹⁴ Christopher Null, ‘Hello, I’m Mr. Null. My Name Makes Me Invisible To Computers’, Wired, November 2015

⁹⁵ Amanda Holpuch, Facebook still suspends Native Americans over ‘real name’ policy, The Guardian, 16 Feb 2015

⁹⁶ Zoe Cat, My name is only real enough to work at Facebook, not to use on the site, Medium, 27 June 2015

⁹⁷ Tessa Sanders et al, Internet Sex Work: Beyond the Gaze, Springer International Publishing, 2017

⁹⁸ Oliver L Haimson and Anna Lauren Hoffmann, ‘Constructing and enforcing “authentic” identity online: Facebook, real names and non-normative identities’, 2016

⁹⁹ The World Bank, ‘1.1 billion “invisible” people without ID are Priority for new high level Advisory Council on Identification for development’, October 2017

¹⁰⁰ See for example, ‘Digital ID solutions for Mobiles by Gravity’

¹⁰¹ Russ Jaskalin, Inside the Jordan Refugee Camp that Runs on Blockchain, MIT Technology Review, 12 April 2018

¹⁰² David Golumbia, The Politics of Bitcoin: Software as Right-Wing Extremism, (University of Minnesota Press) 2016

¹⁰³ Isaac Stanley Becker, ‘New Zealand’s ‘digital strip searches’: Give border agents your passwords or risk a \$5,000 fine’, Washington Post, 2 October 2018

¹⁰⁴ Suzanne Barlyn, ‘Strap on the Fitbit: John Hancock to sell only interactive life insurance’, Reuters, 19 September 2018

¹⁰⁵ A. Drewnowski, ‘Poverty and obesity: the role of energy density and energy costs’, 2004

¹⁰⁶ You Snooze, You Lose: Insurers Make the Old Adage Literally True, ProPublica, 21 November 2018

¹⁰⁷ Location Data Says It All: Staying at Home During Coronavirus Is a Luxury, New York Times, 3 April 2020.

¹⁰⁸ Kate Conger, Richard Fausset and Serge F. Kovalski, ‘San Francisco Bans Facial Recognition Technology’, New York Times, 14 May 2019

¹⁰⁹ Sarah Wu, ‘Somerville City Council passes facial recognition ban’, Boston Globe, 27 June 2019

¹¹⁰ Sarah Ravani, ‘Oakland bans use of facial recognition technology, citing bias concerns’, San Francisco Chronicle, 17 July 2019

¹¹¹ Os Keyes, The Bones We Leave Behind, Real Life Magazine October 2019 issue.

¹¹² ‘Catfishing’ is a colloquial term used to describe the practice of luring a person into an online relationship using a fake persona.

¹¹³ Simply Secure’s research led to an open discussion of catfishing techniques by police targeting research subjects. See also Barton Gellman and Sam Adler-Bell, The Disparate Impact of Surveillance, The Century Foundation, 2017.

¹¹⁴ See for example the work of Helen Nissenbaum, Julia Angwin, Kate Crawford, Mireille Hildebrandt or Antoinette Rouvroy.

¹¹⁵ See Tactical Tech’s research: Varoon Bashyakarla, Psychometric Profiling: Persuasion by Personality, Our Data Our Selves, 2018

¹¹⁶ See for example Facebook Selfie, which gives Facebook users the ability to see their profile how Facebook may see it.

¹¹⁷ See Cathy O’Neil’s Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (Crown Random House, 2016) and Julia Angwin’s Dragnet Nation: A Quest for Privacy Security and Freedom in a World of Relentless Surveillance (Times Books, 2014)

¹¹⁸ See Lisa Rein, ‘Gay man sues Library of Congress, alleging discrimination’, Washington Post, 22 August 2012 and Andrew Liptak, ‘The US government alleges Facebook enabled housing ads discrimination,’ The Verge, 19 August 2018

¹¹⁹ See The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Shoshana Zuboff, 2019.

¹²⁰ Amy Guy, The Presentation of Self on a Decentralised Web, University of Edinburgh, 2017

¹²¹ Elliott and Brody, ‘Straight Talk: New Yorkers on Mobile Messaging and Implications for Privacy’, 2015

¹²² Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Production Regulation)

¹²³ Mireille Hildebrandt and Antoinette Rouvroy (eds), Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology, (Oxford: Routledge) 2011

¹²⁴ Straight Talk’s section on physical environments.

¹²⁵ Eubanks, Automating Inequality

¹²⁶ Sean Illing, ‘How big data is helping states kick poor people off welfare’, Vox, 6 February 2018

¹²⁷ Gary Cohn: Coronavirus is speeding up the disappearance of cash, Financial Times, 29 April 2020.

¹²⁸ Australian Government Department of Social Services, Cashless Debit Card Program, 2018

¹²⁹ <http://www.abc.net.au/news/2018-05-15/cashless-welfare-card-causes-horrible-financial-stress-users-say/9738954>

¹³⁰ Virginia Eubanks, Automating Inequality

¹³¹ Brandon Reynolds, Medium post, 24 August

¹³² Sally Whyte, ‘Employers to give earnings data straight to Centrelink’, The Canberra Times, 7 June 2018

¹³³ Paul Karp and Christopher Knaus, ‘Centrelink Robodebt program accused of enforcing illegal debts’, The Guardian, 4 April 2018

¹³⁴ Jessica Black, ‘Disability advocates hold fears for mental health, suicide’, The Courier, 18 Jan 2017

¹³⁵ Parliament of Australia, Report on Social Welfare System, 2017

¹³⁶ Jay Watts, ‘No wonder people on benefits live in fear. Supermarkets spy on them now.’ The Guardian, 31 May 2018

¹³⁷ Robodebt class action to go ahead despite overhaul of Centrelink debt recovery, The Guardian, 20 November 2019

¹³⁸ See: The Blockchain Open Loop Cash Transfer Pilot Project, a collaboration between the International Federation of the Red Cross and Red Crescent Societies and the Kenyan Red Cross.

¹³⁹ Red Cross Developing Blockchain-Based Currency for Aid Distribution, Asia Blockchain Review, 5 December 2019

¹⁴⁰ Ben Popper, How the NYPD is using social media to put Harlem teens behind bars, The Verge, 10 December 2014

¹⁴¹ UK Department of Education, The Prevent duty, June 2015

¹⁴² When Spies Come Home, an investigative series by Joseph Cox into domestic interpersonal malware-facilitated surveillance, Motherboard

¹⁴³ Tactical Tech carried out a two-year project entitled Sex Workers Voices researching and examining the use of mobile phones for documenting violence in the community

¹⁴⁴ Sanders et al, Internet Sex Work: Beyond the Gaze

¹⁴⁵ For Nextdoor, Eliminating Racism Is No Quick Fix, Wired, 16 February 2017

¹⁴⁶ Banned crime reporting app Vigilante returns as Citizen, says its ‘report incident’ feature will be pulled, TechCrunch, 10 March 2017

¹⁴⁷ Citizen, the real-time crime alerting app, is growing in big cities, CNN, 12 March 2017

¹⁴⁸ See for example, Filming Protests, demonstrations and police conduct, Witness.org.

¹⁴⁹ Obscuracam

¹⁵⁰ Amazon’s Ring Planned Neighborhood “Watch Lists” Built on Facial Recognition, The Intercept, 26 November 2019

¹⁵¹ Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns, The Washington Post, 29 August 2019

¹⁵² See for example, Nellie Bowles, ‘Thermostats, Locks and Lights: Digital Tools of Domestic Abuse’, New York Times, 23 June 2018

¹⁵³ Browser Market Share Worldwide, September 2018

¹⁵⁴ Deepa Seetharanam, Facebook Removes data security app from Apple Store, Wall Street Journal, 22 August 2018

¹⁵⁵ Jack Wallen, Why Opera VPN Isn’t the Mobile Security Solution You Should Be Using, Tech Republic, 12 September 2017

¹⁵⁶ Observations from Tactical Tech’s ‘The Devil is in the Default’ workshops

¹⁵⁷ Aldhaffer, N., Watson, C., & Sajeev, A. Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices. International Journal of Security, Privacy and Trust Management, 2013

¹⁵⁸ Jared Spool, ‘Do users change their settings?’ 2011. <https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/>. This study looked at Microsoft Word’s default settings.

¹⁵⁹ Jialiu Lin, Bin Liu, Norman Sadeh, Jason I. Hong, Modeling Users’ Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings; School of Computer Science, Carnegie Mellon University, 2014

¹⁶⁰ See the 7 principles of Privacy-by-design: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

¹⁶¹ Preliminary conversations with relief agencies confirmed anecdotes of mobiles acting as a kind of currency in communities, with those with access ‘renting’ out and trading access to large groups of temporary users.

¹⁶² For example, Apple’s support document for migrating an Apple ID to a new country.

¹⁶³ See, Wendy Chun, Updating to Remain the Same, (The MIT Press) 2016.

¹⁶⁴ See Tactical Tech’s research on Digital security in context - learning how human rights defenders adopt digital security practices

¹⁶⁵ See for example, Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech, Sara Wachter-Boettcher, 2017

¹⁶⁶ Xuefeng Zhao, Niannian Wang, Ruicong Han, Botao Xie, Yan Yu, Mingchu L, JinpingOu, ‘Urban infrastructure safety system based on mobile crowdsensing’, International Journal of Disaster Risk Reduction, Volume 27, March 2018

¹⁶⁷ See for example, Tomoya Kitazato et al, ‘Detection of Pedestrian Flow Using Mobile devices for Evacuation Guiding in Disaster, 2018

¹⁶⁸ See for example, an overview of technology developments in the sector, in Extreme Tactical Dynamics, 14 March 2018

¹⁶⁹ Linnet Taylor, No place to hide: The ethics and analytics of tracking mobility using mobile phone data, 2014,

¹⁷⁰ Natasha Lomas, Facebook’s Safety Check is a Stress-Inducing Flip of Social Norms, TechCrunch, 14 June 2017

¹⁷¹ Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism, (Public Affairs Books) 2013

¹⁷² See Efficiency and Madness

¹⁷³ The death of Molly Russell led to the introduction of the Age Appropriate Design Code in the UK. See, for example The tech giants pushed Molly Russell towards her death. Now she’s changing the digital world, The Times, 26 January 2020.

¹⁷⁴ See: Stephanie Hankey and Marek Tuszynski, Efficiency and Madness, 2017; Cade Diehm, On Weaponised Design, 2017; and Sara Wachter-Boettcher, Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech, (New York: W.W. Norton & Co) 2017.

¹⁷⁵ Peter Nagy, Gina Neff, Imagined Affordance: Reconstructing a Keyword for Communication Theory, September 2015

¹⁷⁶ See for example Fabricio Teixeira, Diversity by Design: Our role in shaping a more inclusive industry, Medium, 1 June 2017

¹⁷⁷ Clay Spinuzzi, ‘The Methodology of Participatory Design’, Technical Communication, Vol 52, No 2, May 2005.

¹⁷⁸ Trischler, Pervan, Kelly and Scott, ‘The Value of Codesign: The effect of customer involvement in service design teams’, Journal of Service Research, Vol 21, Issue 1, February 2018

¹⁷⁹ See for example: Hannah Devlin, ‘Do no harm, don’t discriminate: official guidance issued on robot ethics’, The Guardian, 18 September 2016 and Eric Amiani Kiruhura, ‘Do no harm: The role and impact of information and communication technologies in delivery of human assistance, Oxford Brooks University, September 2016.

¹⁸⁰ Batya Friedman, David Hendry and Alan Borning, A Survey of Value Sensitive Design Methods, Foundations and Trends in Human-Computer Interaction, 2017

¹⁸¹ See Envisioning Cards

¹⁸² See A Systems Thinking Model: The Iceberg, Northwest Earth Institute

¹⁸³ See Artefact Group’s The Tarot Cards of Tech

¹⁸⁴ Jocelyn Wyatt, The Designer’s Toolkit for Tacking Tough Problems, IDEO.org

¹⁸⁵ See Cassie Robinson’s post on 7 types of Design ‘Beyond Human Centred Design’.

¹⁸⁶ See for example the Circular Design Guide produced in collaboration with the Ellen Macarthur Foundation and IDEO.

¹⁸⁷ See Sheila Jasanoff, The Ethics of Invention: Technology and the Human Future, (New York: W.W. Norton & Co) 2016

¹⁸⁸ See for example, On Weaponised Design, Cade Diehm and references within that text.

¹⁸⁹ Framework for Responsible Data Protection Regulation, Google public document, September 2018

¹⁹⁰ The Age Appropriate Design Code, by the ICO.

