# Make Yourself at Phone: Reimagining Mobile Interaction Architectures With Emergent Users

**Simon Robinson,**[1] **Jennifer Pearson,**[1] **Thomas Reitmaier,**[1]
**Shashank Ahire,**[2] **Matt Jones**[1]

[1] FIT Lab, Swansea University, UK
{ s.n.w.robinson, j.pearson, thomas.reitmaier, matt.jones } @swansea.ac.uk

[2] Industrial Design Centre, IIT Bombay, Mumbai, India
ahire.shashank@iitb.ac.in

## ABSTRACT

We present APPropriate – a novel mobile design to allow users to temporarily annex any Android device for their own use. APPropriate is a small, cheap storage pod, designed to be easily carried in a pocket or hidden within clothing. Its purpose is simple: to hold a copy of the local content an owner has on their mobile, liberating them from carrying a phone, or allowing them to use another device that provides advantages over their own. Picking up another device when carrying APPropriate transfers all pertinent content to the borrowed device (using local no-cost WiFi from the APPropriate device), transforming it to give the impression that they are using their own phone. While APPropriate is useful for a wide range of contexts, the design was envisaged through a co-design process with resource-constrained emergent users in three countries. Lab studies and a subsequent deployment on participants' own devices identified key benefits of the approach in these contexts, including for security, resource sharing, and privacy.

### Author Keywords

Mobile devices, sharing, security, cloudlets, emergent users.

### ACM Classification Keywords

H.5.2 User Interfaces: Input devices and strategies; H.5.3 Group and Organization Interfaces: Collaborative computing.

## INTRODUCTION

Imagine not having access to your mobile phone and needing to make a call. Perhaps you left it at home, its battery is dead, or its screen is broken. Would you borrow someone else's device—perhaps your partner's, friend's, co-worker's, or even a stranger's—to make that phone call? Would you let them use yours if the situation were reversed? This thought experiment is meant to highlight that when we hand over our unlocked phones, we are also handing over a trove of personal data (photos, messages, call-logs, and so on) that we store on the device, and access to personal (Facebook, SnapChat) and business-sensitive (Outlook, Google Drive) remote services that the device provides access to. In some social situations with especially close relationships this is precisely the point of sharing phones and the content they store: to show trust and create intimacy [33]. But outside of such intimate partnerships, people often feel uneasy about sharing their phones, like the participants in a previous study [15], who remained physically present 96 % of the times when phone sharing occurred.

These two studies show that there is an *emotional* dimension to the mobile phone, by virtue of the content we store on and access through it, and who we share that content with. But there is also an *economic* dimension, where we might look at the costs of phones and the different resources they provide. Some phones are more expensive than others, have bigger screens, better cameras, or more storage. Phones are also in different states of repair, with a scratched or shattered screen, a loose headphone or power jack, or a battery that can no longer hold a proper charge. Here people might borrow a phone to make a call because they have run out of airtime, to browse the internet because their data-bundle is depleted, or to take a photo using a better camera. Particularly in resource-constrained communities, phone-sharing practices [27, 28] are also about resource-sharing [36] and not just building and maintaining social and community relationships. In addition, a difficult to overlook fact, particularly in resource-constrained, urban settings is the relationship between mobile phones and crime. For instance, the participants in Walton et al.'s study of mobile media sharing practices of young people in Khayelitsha, a township in Cape Town, South Africa, *"experienced chronic insecurity because of high crime rates, and their mobile phones were often targeted in petty theft and more serious crimes"* [36].

Many people see their phones as an essential part of their everyday lives [9, 35], and we of course appreciate that people everywhere think carefully before they share their mobile phones [16], often worry about their personal data [15], and that mobile phone theft is possible anywhere [32]. But in this research we were initially motivated and informed by the needs and desires of "emergent" users [7, 36]. These users are just beginning to get access to lower-end or second-hand smartphones, but face a variety of resource-constraints, do not necessarily have regular access to reliable charging facilities or can not afford constant data connectivity, and are often more security conscious and worried about their safety, and that of their mobile phones, than those in resource-rich contexts.

Over a two-year period, working in close collaboration with several groups of emergent users, we developed the *APPropriate* concept as a reframing of existing mobiles to better suit emergent user contexts. The prototype we constructed is a



*CHI 2018*, April 21–26, 2018, Montreal, QC, Canada.

ACM 978-1-4503-5620-6/18/04...$15.00.
https://doi.org/10.1145/3173574.3173981

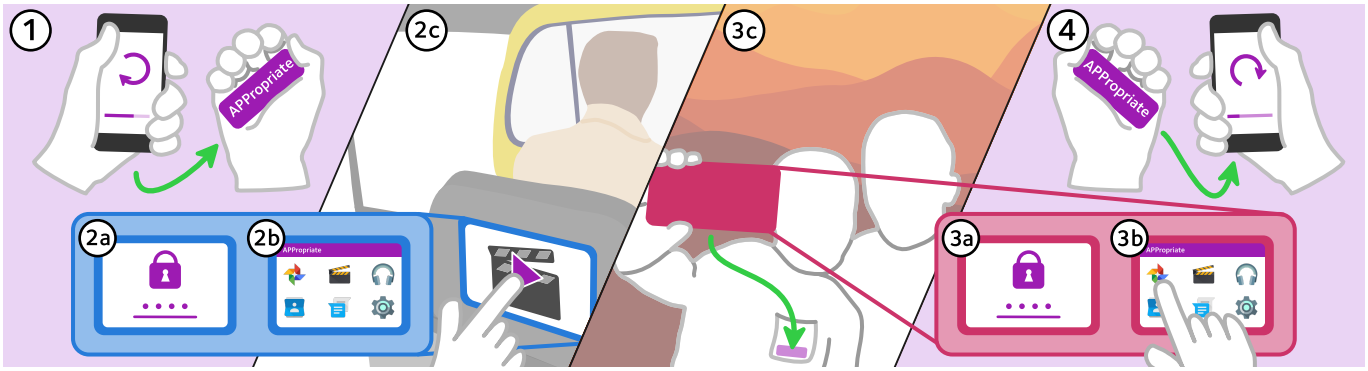


**Figure 1. APPropriate – a small storage device that contains the owner's digital possessions, allowing them to leave their phone behind, but pick up and use any other device at will, as if it were their own. Before leaving home, the user synchronises their phone to the APPropriate (part 1). After doing so, any public or borrowed devices can be appropriated and used at any time (2a–2c and 3a–3c). For example, in part 2, the user is watching a video from their media library on a public display in an autorickshaw. In part 3, the user has borrowed a phone to take a photo – the photo is saved to their APPropriate, and does not remain on the phone. Before they are able to use other devices, the user is prompted for a secret PIN that protects their data (parts 2a and 3a). Entering the correct PIN loads the user's media from the APPropriate, and displays it in the same manner as on their own phone (i.e., in individual apps on a virtual home screen, as in 2b and 3b). Later, back at home, updated media is synchronised back to the owner's phone (part 4).**

small, cheap, portable device that contains a user's mobile content (and, in future, their network connectivity). Importantly, the user's content is held entirely separate from the device used to display and interact with it. This attribute allows APPropriate owners to pick up *any* mobile device, and use it as if it were their own. Figure 1 illustrates the technique's diverse benefits. The design allows security-conscious users to leave their phone in a safe place, but still access their own media via other devices. No internet connection is required. The system also brings other benefits, allowing sharing of devices both when resources are limited (e.g., borrowing airtime but using personal contacts); and, when other devices are more appropriate (e.g., using a higher-quality camera but saving photos privately).

This work is the culmination of a set of ideation workshops, lab studies, and deployments in three countries. In the rest of this paper we explore the activities, studies and interactions that led to the APPropriate concept, and discuss its implementation and novelty, situating it amongst related work. We then present two trials of the system. The first experiment, a simulated-environment study, evaluated the APPropriate concept with groups of emergent users in three different contexts. In the second trial, we deployed the APPropriate in two separate locations for five-week periods. We conclude by discussing the benefits users discovered, and highlighting areas for future work.

## RELATED SYSTEMS AND PERSPECTIVES

In the introduction we have already pointed to some of the rich and nuanced phone sharing practices of users all over the world that form the foundations of this research. Here we position it in relation to software and hardware architectures, both mobile and cloud-based, which separate a mobile device's interface from its storage and connectivity, with a particular focus on the constraints of, and potential benefits for, emergent users. We conclude by engaging with HCI scholarship exploring human orientations to and tensions that arise from data in the cloud.

### Software support

As recently as ten years ago, temporarily borrowing a mobile phone involved nothing more than swapping SIM cards. As smartphones have evolved to become ever more interwoven with the content and the identity of the user, however, such practices have become more strange and distant. In tandem, major mobile manufacturers have made strides towards pushing much of everyday computing to the cloud. The current focus of this change is not on simplifying switching, however; rather, it is either for backup (for occasional use if a phone is lost, or when upgrading devices); or, to access data on additional devices owned by the same person (such as their laptop or tablet). Switching users on a single device is not a simple matter. The iOS operating system, for example, does not have the concept of multiple accounts, so a device must be wiped or restored from a backup to set it up for another user. While Android does have this ability, it is far from seamless. We experimented with setting up and switching to a new account on a medium-end current device (Moto G4; Android 7.0) – the process took just under 5 min and required 25 MB of mobile data. Note also that this accounts solely for logging in to an existing Google account, and does not include synchronising content such as photos, which are downloaded on demand later (if, that is, they have previously been uploaded to a cloud service). In addition, separation of data between the owner and additional accounts is not clean. For example, accounts are able to access (though not delete) all media stored on the phone's SD card. And, while contacts associated with the additional user's Google account are synchronised, their SMS messages are not. Furthermore, accounts are not by default allowed to make or receive calls or SMS messages. Depending on account security settings, logging into a second phone requires the account holder's original device to be physically present to respond to a security alert. The only alternative to this process is to create a guest account, which is a simpler procedure; however, all content created by guest users is permanently deleted when logging out of a borrowed device.

Research into mobile architectures that support disaggregation commonly focuses on the needs of businesspeople [1], or on sharing resources between multiple devices [2, 26], while others have proposed entirely web-based mobile operating systems, offloading computation-heavy aspects [30], or even rendering screen content entirely in the cloud [20], imagining a future in which phones were again "dumb" terminals, kept

constantly up-to-date, and needing only minimal software, rather than hardware updates. Cloud-based systems are attractive for their remote, anytime synchronisation, but also bring drawbacks for emergent users, such as the need for regular (often constant) connectivity. That is, accessing one's media requires a high-bandwidth—and potentially high-cost—internet connection. In emergent user contexts, such connections are often not available or affordable. Our design is very different, in that we aim to allow users to carry with them a part of their device that represents all of their content, then use this as a surrogate for their own phone, allowing them to quickly instantiate and access their own data on any borrowed device.

### Hardware support

There have also been attempts at disaggregation of mobile architectures through hardware-driven designs, which offer a potentially more suitable approach in resource-constrained settings. For example, Google's Ara project [37], now discontinued, was a phone with physically removable components that used a common connectivity framework to allow these to be shared between devices. However, the focus here was not on device sharing, but on sustainability and the ability to upgrade a device without needing to replace its entire hardware. Other designs in this space include, for example, portable devices that can be plugged into compatible tablets or screens to allow users to work on-the-go [12], privacy preserving "live" operating systems [31], "symbiotic" approaches [4], where additional displays can be used in tandem with a mobile device, or recent developments in car and airline entertainment systems that allow passengers to play their own media on fixed screens. Finally, there are parallels with the increasing popularity of mobility as a service, where cars are considered public goods that can be shared across a city. Our design uses a wireless hardware module in order to allow owners to hide the APPropriate when necessary; and, in contrast to in-car or in-flight systems, aims to replicate the entire experience of the user's own device, but does not require the user's phone to be physically present.

### Interaction perspectives

It would be a wasted opportunity to see APPropriate solely as a technological in(ter)vention to address resource or security concerns. Much like the cloud, APPropriate gives users the opportunity to create and access their content on a variety of devices. But, unlike the content we store and share in the cloud, content stored on an APPropriate retains its Gibsonian affordances [10]. This is a topic that Harper and Odom [11] explore as they position people's digital data not as objects or things to be created or accessed, but as a form of digital possession. This concept of possession, in their view, is lost in translation when digital data is stored in the cloud [21], as *"their trust [ . . . ]—that things exist in ways that can be acted on—seems to wane"* [11, p. 285]. In their view, possession requires ownership and control. Consider the participants in Schoon's study of hip hop artists in a South African township [29], and the ways in which they created and shared tracks using an online file-sharing service. Many kept detailed paper records of the URLs of the tracks they uploaded, highlighting how digital objects became valuable possessions. However, the unreliable nature of file-sharing services led some participants to choose instead to carry and hide flash-drives with their tracks on their person.[1] In web or cloud contexts, as Lindley et al. [19] report, ownership is often seen as equivalent to access (e.g., knowing a password), rather than requiring physical possession. The APPropriate design offers a more traditional model of ownership, by physically carrying a wireless storage device, but also offers the opportunity to seamlessly access its contents from numerous new devices. The practices reported by Schoon motivate and showcase potentials for systems like APPropriate to provide cloud-like services, while retaining their Gibsonian affordances that allow people to take stock over, care for, and safekeep their digital possessions.

### Emergent user setting exemplars

While the APPropriate system manifests the creativity, ideas, and enthusiasm of all those involved in its design, it also bears resemblance to other systems imagined and developed in emergent user contexts. Reitmaier et al. [24], for example, proposed "cloudlets" as a different way of thinking about cloud computing in resourced-constrained communities. Cloudlets, in their view, can be thought of as infrastructure independent, hyperlocal and ad-hoc *"instantiations of the cloud that [ . . . ] provide similar services and opportunities for both virtual and physical engagements"* as well as opportunities for *"engaging with co-located people"* [24]. Commercial systems, such as Liberoff and Horn's Movirtu [18] proposed technologies that allow users to *"login and out of any GSM phone"* and access their mobile number, call records, and mobile money. However, our approach focuses on separating digital possessions to a portable that brings both media and identity to any other device.

## DESIGN PROCESS

APPropriate emerged through a multi-year design exercise, involving emergent users throughout to generate a range of concepts and prototypes. A detailed exploration of the initial design process can be found in [14]; here we focus solely on those aspects that inspired and led to the APPropriate design.

### Participatory design workshops

At the start of this research, in June 2015, we carried out a series of participatory design workshops with emergent users in Bangalore, Nairobi and Cape Town, centred around a series of envisioning activities. A total of 49 people took part, with activities involving participants sketching, describing and acting out the ideal mobile devices that they might own in the "far-off future", defined as five-to-ten years ahead. There were no constraints to the tasks, and we did not give examples or suggest use-cases – participants were simply asked to imagine a future mobile device designed specially for them.

Participants in Nairobi and Cape Town generated ideas around camouflaging their devices, or refining the phone's form factor to make it less visible to potential thieves. In their everyday environments, losing one's phone to theft was a common problem. In Bangalore, participants focused more strongly on how future technologies might allow seamless sharing of devices, both in terms of features (for example, to use a better screen when available), or out of necessity (e.g., when low on battery or airtime on one's own device). We built early-stage prototypes of these concepts, feeding into follow-on workshops.

[1] Personal communication with Schoon [29] at AfriCHI '16.

### Future technology workshops

We used the concept prototypes built after the initial workshops as starting points for a second workshop in Cape Town one year later (June 2016). In addition to the concepts from the earlier sessions, we also asked participants to interact with and consider examples of future technologies from both research and commercial perspectives. Over the course of the workshop, then, participants saw and experimented with a wide range of future technologies (both real and conceptual) as inputs to ideation exercises. The aim was for participants to think about new devices that could fit more closely into their lives, combining or adapting the technologies they had seen during the day to create devices that worked especially well for them.

Four distinct design concepts emerged from this process, and we produced scenario sketches and videos of each of these ideas to illustrate their potential use. Following this, we ran a short workshop with the original participants in both Cape Town and Nairobi to critique, refine and select candidate ideas for further refinement and prototyping. Participants watched the four scenario videos, discussing their benefits, drawbacks and potential problems, and then rated each idea's usefulness, ranking the designs in order of preference for development.

The most highly rated design was for a device that separated the storage and networking elements of a mobile phone from its display and interface, allowing the owner to use any other device as their own. Participants in the workshops envisaged this concept as supporting direct sharing of hardware and resources using a single device that embedded aspects of both of the ideas demonstrated in the prototypes from the participatory design workshops. The scenario video for this design explored its benefits with an explicit focus on security (i.e., a custom-built wearable that connects to any phone), and after viewing the video it was clear that participants saw a great deal of benefit in being able to leave their phone in a more secure location while on-the-go. For example, comments included: *"it is very useful as it reduces theft"*; *"it is safe"*; and, *"[I] would be free and secure without worrying who is watching"*. In addition, participants also pointed out the advantages of this design for its ability to let people borrow devices from others to temporarily use as if they were their own. In this context, participants saw benefits both for sharing of capabilities (*"I can borrow a camera"*); and, for using another person's device when their own was, for example, low on power (*"my phone may be out of battery charge but with another device I can still be on"*). Finally, participants particularly appreciated the small form factor of the device: *"[it] would almost eliminate the hassle of carrying a phone"* and, *"I would use it – the fact that I can avoid carrying my devices everywhere is a win"*.

## THE FRAMEWORK

It was clear after the workshops that the concept of separating a phone's screen and interface from its storage and networking was highly attractive, and would address several limitations that participants saw in their current devices. Consequently, we developed a prototype APPropriate device and framework as a probe to further explore its potential architecture.

Conceptually, we imagine a consumer-level version of the APPropriate design being able to store and synchronise a range of content types defined by the device manufacturer or phone owner. As an initial probe, we opted to develop part of the scheme's functionality using an Android app and accompanying hardware module, allowing users to interact with media from their own phone on a virtual homescreen when borrowing other devices. The APPropriate hardware is a repurposed wireless storage device, with no interface except a power switch and a status LED. All content synchronisation is handled automatically by the accompanying app.

Figure 1 illustrates typical usage of the APPropriate. When a user wishes to leave their phone behind, their contacts, music, videos, and most recent photos and messages are synchronised to the APPropriate from their phone (see Fig. 1, part 1). When the user would like to interact with their own content using a public or borrowed device, they simply open the APPropriate app on the adopted mobile and enter their secret 4-digit PIN, which triggers automatic synchronisation of their data on to this device (see Fig. 1, parts 2a–2c and 3a–3c). The appropriated device is now transformed to appear as if it were the user's own phone, displaying the apps and background wallpaper from the APPropriate, rather than those native to the borrowed device. Any new media that is created—photos taken, videos recorded or contacts added, for example—are saved to the APPropriate, rather than to the device in actual use.

When finished interacting with the borrowed phone, the user exits the APPropriate app to ensure all of their media is removed from the appropriated device. When the user returns to their own phone, opening the APPropriate app synchronises any updated media from the APPropriate, and the user is able to use and interact with these content items as normal.

We see four interconnected benefits of the approach. When using the APPropriate system to separate their content from the device it is manipulated with, users are able to:

**Share when resources are limited:** For example, borrowing someone else's phone when their own has low battery; using another device's mobile data when their own is depleted.

**Share when better resources are available:** For example, watching a video from their APPropriate on a larger screen; using a higher-quality camera to take photos of their own.

**Increase device and personal security:** The APPropriate is far smaller than a phone, so can easily be hidden away when personal security is an issue, or data backups are needed.

**Increase privacy:** a single phone can be shared between a group of users, but all data is private and PIN-protected.

## EXPLORATORY LAB STUDIES

We conducted a series of lab studies of the APPropriate design in three countries. Our goal was to elicit participants' thoughts and opinions about potential usage, usefulness and suitability of the concept. Each session used the prototype described above, and a simulated environment method. As the system is designed to be used in a variety of locations over a prolonged period of time, in order to test in a controlled manner we adapted the approach described by Kray et al. [17], simulating potential contexts of use by using projected images, videos and audio to give the impression of different locations whilst in the same physical space. Four environments were created: home;

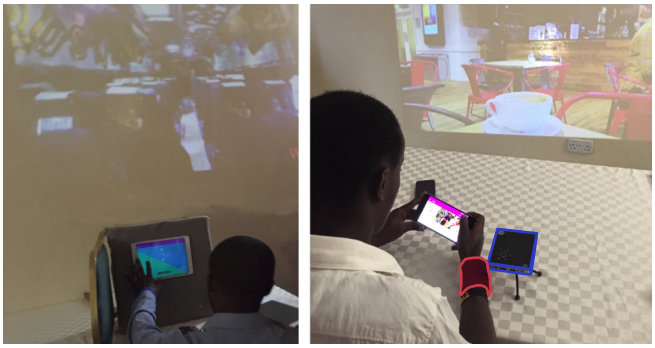

**Figure 2. Two of the simulated contexts as seen in the Nairobi study, for illustration (other contexts and locations are not shown). Left: travel (in this case, a matatu[2]), simulating a tablet attached to the seat in front of the user. Right: public space (a coffee shop), showing also the fitness sweatband used to represent a watch-based APPropriate (highlighted in red), and one of the projectors (blue) used to help simulate each context.**

travel (e.g., minibus, matatu[2] or autorickshaw[2]); public space (e.g., coffee shop or spaza[2]); and, quiet space (e.g., library or study area). Figure 2 illustrates examples of the situations that were simulated. In each space we also placed mobile devices that might be available in that context, depending on the scenario (one to three in each space). These ranged from a large high-quality tablet to a small, compact device, and from a high-end smartphone to a low-cost entry-level smartphone. For example, in the matatu, a tablet was available on the back of the seat in front of the user (Fig. 2, left). In the public space there were three mobiles, imagined to belong to friends who were also there. During the study, participants moved between each of the areas, using the APPropriate device whilst imagining that they were in the place and situation that was simulated.

### Procedure

The study began with an IRB-approved informed consent process, followed by questions about demographics and phone use. We also asked participants about their current behaviours and attitudes toward borrowing and sharing mobile devices. We then demonstrated the APPropriate system. Each participant was given a phone that had been set up as the "home" phone for an APPropriate module. Participants were asked to imagine that this was their own phone, and that the APPropriate was a watch-like accessory. To reinforce this, we asked participants to wear a fitness sweatband on their wrist, and insert the APPropriate device underneath (see Fig. 2, right).

We then interactively demonstrated the APPropriate concept to participants by asking them to swap phones with another person, enter the PIN of their APPropriate into the borrowed device, and then take a photo using this new phone. After doing so, participants exchanged phones again, verifying that the photo they had taken on the first device now appeared on the second. Participants then spent some time swapping devices repeatedly to explore how images, music, videos and SMS messages could be created on any phone, but were visible only to them, and remained only on the APPropriate device.

After this training period, participants were accompanied by a researcher to visit each of the four simulated environments in turn. Each participant visited the four areas in a different order, so that only one participant was present in each place at any time. We explored participants' usage of the APPropriate in each context, and also their choice of devices when multiple options were available. In each place, then, the participant was asked to pick any of the devices that were available, and use the APPropriate to perform one or more tasks as specified by the researcher (e.g., take a photo; watch a video; send a text message, etc.) For example, in the travel area, participants were asked to choose a video to watch, and then reply to a text message. Participants performed these actions while thinking aloud. The researcher observed during this process and, after each task, asked participants to explain the device choice they had made. After all four places had been visited, participants returned to the home space, and discussed the experience.

In a post-task group discussion we asked questions around the system's usefulness (including a Likert-like rating, 1–10; 10 high), potential privacy concerns, its advantages and disadvantages, and broader phone use, including trade-offs of features against privacy, security and cost. The study concluded with a discussion of potential improvements to the system, after which we compensated participants for their time.

[2]Matatu: a shared minibus (Kenya); Autorickshaw: an urban transport vehicle (India); Spaza: an informal convenience store (South Africa).

| | Study location | | |
|---|---|---|---|
| **Participants who** | **Nairobi** | **Mumbai** | **Cape Town** |
| Own a smartphone | 77 % | 87 % | 83 % |
| Have a data plan | 77 % | 33 % | 17 % |
| Share their phone with others | 69 % | 67 % | 50 % |
| Worry about privacy when sharing | 54 % | 47 % | 33 % |
| Worry about theft of their device | 92 % | 33 % | 83 % |

**Table 1. Lab study participants' technology ownership and concerns.**

### Participants, locations and technologies

*Nairobi, Kenya:* We recruited 13 emergent users (7F, 6M, aged 21–29) to take part in the Nairobi trial. There was one group of four participants, and three groups of three people. All participants were blue-collar type workers (e.g., waiters, cleaners, casual labourers, etc.) of mixed educational attainment. Ten participants owned smartphones, with the remaining three owning featurephones. Each participant was given KES1000.

*Mumbai, India:* We recruited 15 emergent users (8F, 7M, aged 19–46) to take part in the Mumbai trial, in five groups of three people. As in Nairobi there were a mix of backgrounds, ranging from students to teachers to housekeepers. Thirteen participants owned smartphones, with two owning featurephones. Each participant was given ₹500 after the study.

*Cape Town, South Africa:* We recruited 6 emergent users (4F, 2M, aged 21–38) to take part in the Cape Town trial. There were two groups of three participants. Three participants were unemployed, with the remainder employed in manual labourer jobs. Five participants owned smartphones, with one owning a featurephone. Each participant was given R200.

#### *Technology ownership and attitudes*

Educational and technological experience levels of the 34 participants varied between locations, but all lived in lower socioeconomic areas. A summary of technology ownership and

attitudes towards mobile devices is shown in Table 1. Although the majority of participants owned a smartphone, it was often not a *personal* device; i.e., as is common in emergent user communities, sharing was common. In Nairobi, Mumbai and Cape Town, respectively, 69 %, 67 % and 50 % of participants shared their device with someone else. Subscribing to a regular data plan was also not commonplace in two of the locations (only 33 % of participants in Mumbai and 17 % in Cape Town paid for an internet connection on their device). As previously discussed (cf [27, 28, 36]), this type of shared device use and ownership is in stark contrast to traditional users (in, say, metropolitan San Francisco), who have enjoyed uninterrupted data use and truly personal devices for many years.

Differences in attitudes to device security and privacy between locations are also highlighted in Table 1. There was a correlation between participants sharing phones and whether or not they were worried about the privacy of their data. Specifically, participants were 40 % more likely to be worried about the privacy of data on their device if they regularly shared it with someone else. Worries relating to the security of devices varied significantly across the three sites. In particular, participants in both Kenya and South Africa were extremely worried about security, with 92 % in Nairobi and 83 % in Cape Town stating that they would not feel comfortable using a phone in public for fear of it being a target for robbery. These responses show the potential value APPropriate could offer in these contexts.

### Results

Turning now to core results from each location, where we highlight findings around acceptance and the value of APPropriate.

#### *Nairobi, Kenya*

Participants in Nairobi were very positive about the APPropriate concept, with the majority of their feedback focusing on the benefits the design offered in terms of security (a major concern for 92 % of Nairobi participants, as the pre-study interviews highlighted). The fact that the device was small and easily hideable was seen as a positive aspect for many, with one stating, for example: *"I'm worried about pickpocketing on the matatu, but this is good; carrying a phone is dangerous, and this is smaller and easier to carry,"* and another commenting: *"[it is] very useful to me because where I live phones get stolen [often], so moving around without people knowing what you're carrying is great"*. Others appreciated that the device did not look like a phone, and so might be less likely to attract attention: *"it's flexible – you can go with it anywhere without anyone recognising it's a phone, so it wont be stolen, so you can walk with it anywhere even at night"*. Participants also saw privacy benefits of the approach, both for shared phone use, and for general concerns: *"it improves my privacy – unless I give out my password the safety of the phone is improved"*.

Other participants saw opportunities to further refine the design: *"[it is] too big and uncomfortable – I'd like it very tiny, and inside my skin,"* and its security: *"can it be hacked?"*. Overall, however, the APPropriate prototype was very well received, with an average usefulness score of 8.8 out of 10. All participants would use the device if it were commercially available. Of course, we are, like Dell et al. [6], sceptical of high scores and potential bias when evaluating systems with emergent users, particularly in lab settings, but can see both in comments and observations how participants were linking APPropriate into their everyday practices and use of mobiles.

#### *Mumbai, India*

Participants in Mumbai were less focused on security than those in Nairobi or Cape Town, and saw more benefits in scenarios where devices were forgotten, damaged, shared, or lacking features. For example, while moving from place to place to use the system, participants actively chose larger devices to take photos or view videos, citing screen size as their motivation. Other potential benefits of the sharing that the system enables were mentioned – for instance, one participant said: *"there's no need for a phone – even if you forget it your data is still in your pocket,"* while another stated: *"if there is an occasion when I don't have a good cellphone I can borrow someone else's to take a photo and get it into my [APPropriate]."*. Further suggestions included sharing phones to gain access to better speakers, devices with charged batteries, higher-quality cameras, or simply those that looked more attractive.

Privacy concerns were also evident in this group, as summarised by one participant: *"I liked the concept of entering a code and synchronising [ . . . ] so nobody else can see the data,"* while another noted: *"I like the security aspect – you have a password to enter and it is secure"*. Similar to those in Nairobi, some participants had reservations regarding the form of the prototype, mainly due to the fact that it was attached to their wrist under a fitness band in a temporary manner. Suggestions for improving this aspect included attaching the device discreetly under a belt, or changing its form factor to be more *"watch-shaped"*. Concerns over the security of the APPropriate should it get lost were also noted, and several participants forgot to disconnect from the device before switching to use a different phone, causing slight confusion. Overall, participants in Mumbai were very positive about APPropriate, with an average of 9.9 out of 10 for usefulness, and a unanimous "yes" vote for whether they would use it were it generally available.

#### *Cape Town, South Africa*

Similar to Nairobi, participants in Cape Town focused heavily on the benefits of APPropriate for security. For instance, one said: *"you can leave your phone at home – good for the criminals, they won't rob you,"* while another noted: *"it is very very great, because it is more safe in terms of your phone; because you can leave it behind, it saves your phone from getting robbed or stolen"*. There were also comments relating to the privacy of data when using a shared phone (as 69 % did): *"it would be useful to save my personal stuff; information I did not want people to see,"* and: *"the best thing is that your privacy is with you – it won't be accessed by anyone else"*.

Another benefit mentioned by this group was the ability to share resources, primarily focusing on sharing of airtime. For example, one participant stated: *"[it is] useful because sometimes you just need to send an SMS from someone else's phone,"* while another said: *"as long as I have the [APPropriate] I can use someone else's phone; it doesn't even have to belong to me"*. All participants responded that they would be very likely to use the APPropriate if it was commercially available, and gave an average score of 8.7 out of 10 for its usefulness.

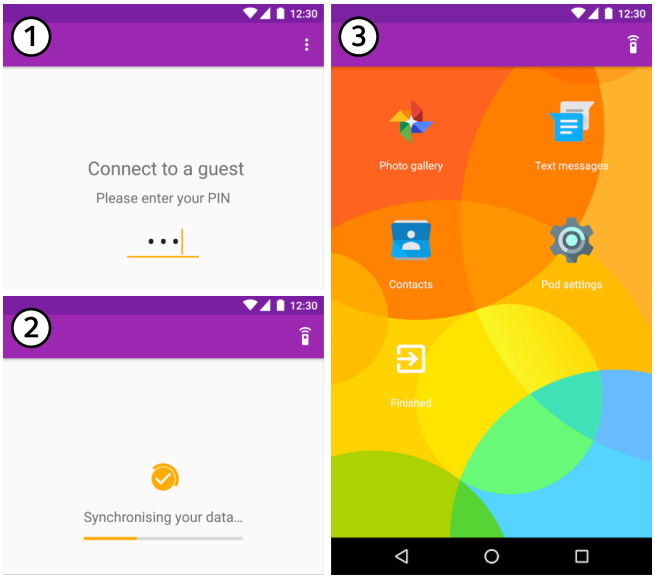


**Figure 3. The APPropriate app interface on a borrowed phone. Picking up any APPropriate-enabled Android device prompts for a PIN (image 1). Entering the correct PIN authenticates with the user's APPropriate module and synchronises their content (2), presenting as closely as possible the same experience (photos, SMS messages, contacts and wallpaper) that the user is familiar with on their own smartphone (3).**

## LONGITUDINAL DEPLOYMENTS

It was clear after the lab studies that the functionality provided by APPropriate was highly desired, and that the system as designed would address several of the limitations that the emergent users we worked with saw in current mobile devices. Consequently, we further refined the prototype based on study feedback, and created a version of the hardware module and accompanying Android app[3] that could be deployed for trials in conjunction with users' own mobile devices. We deployed the APPropriate prototype in Cape Town and Mumbai with groups of emergent users, including several of those who originally participated in the earlier phases of the design process.

### Prototype refinements

We refined the lab study APPropriate probe in order to ready it for deployment on users' own phones. After extensive research, we concluded that moving the SIM card to the APPropriate itself to allow full separation of interface and content was infeasible for a deployment using participants' own devices. Taking a SIM-driven approach would require significant engineering effort to extract the telephone network functionality from the core Android platform into an external device; and, more importantly, would require handing out phones to participants rather than extending the existing ecosystem of devices that they own and are familiar with. Instead, we expanded the prototype's synchronisation method to work directly with photos, contacts and SMS messages in standard apps. This allowed us to deploy and test as fully as possible the concept that the participatory design workshop participants had envisaged, with the exception of remote SMS and phone calls. We felt that the trade-off of this aspect for compatibility with participants' existing devices was especially worthwhile.

[3]Toolkit source code (MIT licensed), documentation and further technical details available at: https://github.com/reshaping-the-future/pod

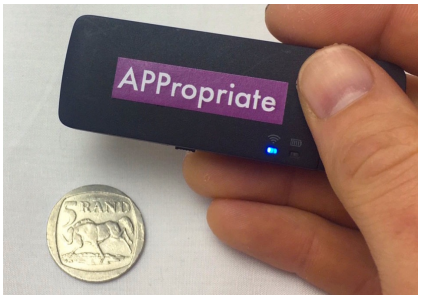


**Figure 4. The APPropriate hardware, with a 5 Rand coin for scale. A switch on the side of the device (next to the user's fingertip in the photo) toggles its inbuilt WiFi on and off. The blue light in the image flashes on startup, then goes constant once ready to sync.**

The deployed app and hardware module are shown in Figs. 3 and 4. As in the lab study, opening the app initiates a search for nearby APPropriate devices and, if found, automatically authenticates to and synchronises content with the user's own APPropriate. Alternatively, the user can enter a PIN to connect to other nearby devices. After connecting to their APPropriate, the phone synchronises the user's contact list and most recent photos and SMS conversations. All contacts are synchronised each time. The number of images and SMS conversations copied from the user's own phone to the APPropriate is configurable from 2 to 30, with the most recent items selected first (limited primarily to ensure that synchronisation completes quickly). There is no limit to the number of items that can be saved to the APPropriate when using it on a borrowed device.

Content on a borrowed device is presented as shown in Fig. 3 (3). When capturing or browsing photos, interaction is exactly as on the user's own phone. Interaction is slightly different when using functionality that requires telephone network access, due to our decision to make the deployed APPropriate compatible with existing mobile devices. Contacts can be viewed and edited as normal, but calling a contact will use the airtime of the borrowed device, and originate from that telephone number rather than the user's own number. When sending SMS messages, users are given the option to either send immediately, using the borrowed device's airtime (and from the phone number of that device), or queue for delivery when the user returns to their own phone (cf. [13]). This trade-off increases compatibility, but reduces personalisation – we envisage a future version of the system as a self-contained SIM- or virtual SIM-enabled device that can be accessed and controlled by any APPropriate-compatible screen or smartphone.

To disconnect the borrowed device from their APPropriate, the user touches the button labelled "Finished" (lower left in Fig. 3 (3)). To address the privacy concerns raised by participants in the lab studies (Mumbai), we encrypted the contacts and SMS messages stored on the device, and added a range limit. That is, if the APPropriate hardware goes out of range of a borrowed phone, their content is removed from that phone, ensuring that the user's privacy is preserved. Guest content is only ever stored in the app's private cache (only potentially visible to the Android OS, not other apps), and is permanently deleted when users disconnect. Despite suggestions from some participants for the device to be more "watch-shaped" (Mumbai), we chose to diverge slightly from the studied design in favour of a sleeker stick-like form. This decision was primarily so users could hide the device anywhere they saw fit (as Nairobi and Cape Town lab study participants requested), rather than being constrained by the physical form factor of a wrist-worn design.

## Method

We recruited 32 participants from two countries to take part in five-week deployments of APPropriate. The deployment began with an initial set-up meeting, followed by three follow-up meetings, scheduled to take place 1-week, 2-weeks and 5-weeks after the initial session. Participants were recruited in friendship groups of 4–5 people, in order to ensure that users had the possibility to access other devices to view or edit content. To gather different perspectives on the design, we performed the study with two distinct groups of emergent users, each with a different focus. The deployment in Cape Town (16 participants) had a security focus, while that in Mumbai (16 participants) had a device sharing focus. Table 2 illustrates the differences in attitudes to mobile devices between the cohorts.

Due to these different focus areas, there was a slight difference in the behaviour of the APPropriate between the two deployments. Specifically, in the security-focused deployment, each participant's APPropriate device had a "home" phone (i.e., the participant's own device), as illustrated in the scenario in Fig. 1. In the sharing-focused deployment, however, we altered the system so that each APPropriate was a standalone device, and would therefore behave as a "guest" on every phone it was used with. For example, three people in the same family sharing one phone would all have their own APPropriate, and would use it to "log on" to the shared phone to make it appear as their own. We made this decision to mimic how the system would behave for multiple users sharing a single phone, as this behaviour is more common amongst the Mumbai participants.

A prerequisite across both sites was that participants must own, or have regular access to, an Android phone (Gingerbread (v2.3) or later). In Mumbai, due to the device sharing focus, there was an additional requirement that participants must regularly share this phone with someone else (see Table 2).

The metrics of the deployment were primarily qualitative responses gathered via one-to-one questioning at each follow-up session, but there were also a small number of quantitative ratings (see Table 3). All participants' comments, suggestions and ideas were transcribed, translated to English (where required) and stored in spreadsheets for later analysis. Analysis was undertaken primarily via clustering of themes by two researchers (first thematically, then cross-validated). We also logged usage of the system via its accompanying app, but kept this to a minimum in order to preserve participants' privacy. The app recorded only the duration and number of times it was connected to a phone to display the user's information. At the end of the final two follow-up sessions, each participant could choose (or decline) to share these logs with the research team for analysis.

## Procedure

Each deployment began in a meeting with each group, After an IRB-approved informed consent process, we began with individual questionnaires to gather demographic information, and probed participants' current phone use and attitudes towards their devices. This was followed by a demonstration of APPropriate, and, if participants owned a compatible phone, installation of the accompanying app. Each participant was then given their own APPropriate module, and was shown how to change its PIN, and how to select which media items they would like to synchronise. As part of the briefing we explicitly informed participants about the security of the system (i.e., content privacy and deletion) and its PIN-protected access. Participants were then encouraged to experiment with the technology—borrowing other group members' phones, transforming into their own, then returning, and so on—until they were comfortable with its use. This initial session lasted around 45 min.

| | Study location | |
|---|---|---|
| **Participants who** | **Cape Town** | **Mumbai** |
| Share their phone with others | 38 % | 100 % |
| Worry about privacy when sharing | 19 % | 75 % |
| Worry about theft of their device | 93 % | 38 % |

**Table 2. Longitudinal deployment participants' attitudes towards their devices. Those in Mumbai shared their devices with other people more than those in Cape Town, and were more worried about data privacy, perhaps as a result of this behaviour. Users in Cape Town were far more concerned about the physical security of their phones (i.e., risk of theft).**

For the next five weeks of the study, participants were asked to "borrow" another person's phone (i.e., another study participant's device) at least three times per week. At the first follow-up meeting we revisited the APPropriate usage process to ensure participants were comfortable with this, and asked for feedback on the system's usefulness and reliability (both Likert-like (see Table 3) and subjective), and any suggestions for improvements or issues that needed addressing. The second and third follow-up meetings were intended to gather more nuanced feedback about the design, and focused on participants' usage, and the aspects of the system's design that were particularly suited to their everyday lives. After each session, participants were given R250 (Cape Town) or ₹500 (Mumbai) as a token of our appreciation for their continued participation. At the end of the study, participants kept the APPropriate in order to allow them to continue using it if desired (though we did not track this behaviour, in order to preserve privacy).

### *Security focus: Cape Town, South Africa*

We recruited 16 participants (10M; 6F, aged 19–26) from Langa—a township near Cape Town, South Africa—to take part in the security-focused deployment. There were four friendship groups (four people in each group), and all participants owned a smartphone. Participants were mainly students (50 %) or unemployed (44 %), and 63 % had access to either a laptop or a tablet PC in addition to their smartphone, while 38 % of participants shared their phone with someone else. Most participants (93 %) were worried about the security of their devices, but few (19 %) were concerned about the privacy of their data (e.g., their personal messages, photos etc.).

### *Device sharing focus: Mumbai, India*

We recruited 16 participants (14M; 2F, aged 18–46) from slum areas in Mumbai, India to take part in the device sharing-focused deployment. Most participants were housekeepers (75 %); other occupations included delivery driver, mechanic and student. As in Cape Town there were four friendship groups (four participants per group). While all participants owned a personal smartphone, two were very old devices that were not compatible with APPropriate. All participants shared their phone with someone else (on average, with 3.8 others,

| How useful is APPropriate for | Study location | |
|---|---|---|
| | Cape Town | Mumbai |
| Allowing you to leave your phone at home | 8.6 | 8.5 |
| Phone sharing purposes | 9.1 | 9.0 |
| Security purposes | 9.4 | 6.4 |

**Table 3. Average scores given by participants in the initial follow-up sessions of the longitudinal deployments (1–10; 10 high).**

mostly family members), or regularly used other people's devices. Access to additional technology was lower than in Cape Town: only 13 % of Mumbai participants had access to a laptop or tablet computer as well as their primary device. Participants were less concerned about physical device security than those in Cape Town, but 75 % worried about the privacy of their data, possibly as a result of their phone sharing habits.

## Results

Table 3 shows the average scores from the initial follow-up session of each deployment. These promising results show particularly high ratings for the usefulness of the APPropriate system for phone sharing purposes (9.1 and 9.0 out of 10 in Cape Town and Mumbai, respectively). As might be expected given the different context of the groups, participants in Cape Town felt the technology was more useful for security than the Mumbai group. In both locations, although we only asked participants to use the device three times per week, many used it more often (5.8 times per week on average across both sites).

After five weeks of use, 13 of the 16 Cape Town participants[4] and all of the 16 Mumbai participants returned for the final follow-up session and exit interview. Overall, it was clear that APPropriate had been particularly well received by the majority of participants, with 11 of 13 from Cape Town and all 16 from Mumbai stating that they wanted to keep using the device and its accompanying app after the study concluded.

### *Security focus: Cape Town, South Africa*

In discussions, the majority of participants from Cape Town focused on the security aspect of the design, giving comments such as: *"I can leave my phone at home, the [APPropriate] I can hide and the criminals won't see it," "I'm less prone to criminals and less chance of getting robbed"*. When asked if they felt that the APPropriate hardware was a desirable item for thieves, 64 % of the Cape Town participants felt that it was not, with the remainder stating that the device was less vulnerable to theft than a phone: *"in the society we live in people would probably take it – [APPropriate] puts me in less danger than a phone, though,"* and *"considering the place I live in, it is stealable – it's less stealable than a phone though"*.

Cape Town participants were also keen on APPropriate's resource sharing ability. Some, for example, enjoyed making use of others' cameras for higher-quality photos: *"my phone doesn't take nice pictures, so I'd borrow one and it would be on my phone later,"* and *"it was my birthday and I used my sister's nice phone to take pictures and sent them to my phone via the [APPropriate], so it helped me get good pictures"*. Others used the system to share a data or cellular connection: *"it let me send text messages using someone else's airtime – it's easier for me as I don't normally have airtime"*. Issues relating to power were also experienced and resolved via the APPropriate: *"my battery was dying [ . . . ] the number was on my [APPropriate], so I used [P5]'s phone to call",* and *"electricity went out for a week during the storm so I couldn't charge my phone – I could still borrow a phone with charge, though"*.

It became apparent in the follow up sessions that several participants had been downloading or transferring the app onto family and friends' devices (i.e., those not taking part in the study) so that they could make use of their APPropriate device when other study members were not present: *"I was in Khayelitsha with no airtime, so I installed the app to my uncle's phone and made the call"*. There were also reports of family and friends' eagerness to own an APPropriate device of their own: *"I explained it to my family – they were very curious about when it will be available to everyone,"* and *"my big sister wants the app but there's only one [APPropriate], and it's mine"*.

### *Device sharing focus: Mumbai, India*

Mumbai participants' comments tended to focus more on situations when they had either forgotten their phone (e.g., *"my phone was at home so I used the [APPropriate] for calling from a colleague's phone"*), when someone else in the family was using it (e.g., *"kids were using the phone so I took the [APPropriate] to my brother-in-law's place and used it for taking pics during festive time"*), or if their own phone was damaged (e.g., *"when my phone is broken I can use another"*).

Participants spoke of phone battery issues (e.g., *"my mobile battery was not working for four days so I used [APPropriate] on another device to use the camera and for calling"*), as well as a lack of airtime (e.g., *"I did not have balance but I called the person by using another cell phone and my [APPropriate]"*) that were overcome by using APPropriate. One even spoke of an occasion where their phone was accidentally erased, but they were able to restore media using their APPropriate: *"images from a recent picnic were in my [APPropriate ] and next day my mobile was formatted so the data was saved"*.

### *Usage*

By the end of the study we were able to recover complete logs from 14 participants in Cape Town and 10 in Mumbai. The remaining logs were either lost or incomplete for various reasons, including people switching phones during the study because their original phone was lost or stolen, or borrowed by another family member. Another common reason was that participants had deleted the APPropriate app from their phone to make space for other apps, then reinstalled it when they wanted to use it, unwittingly deleting logs of previous use in the process.

Turning first to the security-focused group in Cape Town, the average number of times an APPropriate device was used on a borrowed phone was 24 (min: 5, max: 50). The average number of times each participant's own phone was used by a guest APPropriate device was 8 (min: 1; max: 21). Note that this usage level is higher than the minimum number of times we

[4]One participant was unable to attend due to travel for family reasons; another was uncontactable by researchers or other group members. The final participant misplaced the APPropriate hardware after the third meeting, and decided not to attend the final meeting as a result. There were at least three participants present in each of the groups.

suggested participants should use the system (15; three times per week). On average, participants in this group spent 67 s interacting while using guest phones. This duration does not include the time to synchronise data between the APPropriate and the phone, which was 16 s on average. On average, each participant used their APPropriate on 1.4 devices (not including their own; min: 1, max: 6), and each participant's phone was used by 2.6 unique guest APPropriates.

In the device sharing-focused study—where APPropriate devices are guests on all phones—the average number of times each APPropriate device connected to a guest phone was 34. Overall, the average time spent interacting with the system in this group was 50 s, and the average time to synchronise data was 39 s (devices in Mumbai were largely of lower specification than those in Cape Town). On average, each participant used their APPropriate on 1.9 other devices, and each participant's phone was used by 5.7 unique guest APPropriates.

The difference in logged use between own and guest devices in both locations supports comments that participants were downloading the application from the Google Play store or sharing it directly to other phones (i.e., those not involved in the study) and connecting to these via their APPropriate. Indeed, analysis of Play store download logs shows nine downloads in India during the study. Other participants, in particular those in South Africa, recounted sharing the app using phone-to-phone direct sharing services such as ShareIt or Zapya.

In terms of physical appearance, 96 % of participants (over both sites) stated that the device's size was acceptable, with the majority keeping it hidden within a pocket or a bag during use. Some participants suggested that making the device blend in more subtly—perhaps by making it look like a button or zip pull, or even embedding it into a necklace—would make it more secure for the environments in which they live.

## DISCUSSION AND CONCLUSIONS

In many countries, having a mobile phone to-hand makes people feel safer [5]. In other places, however—for instance, in more resource-constrained settings—having a phone on one's person can make someone more of a target for theft [23]. In this work we have developed and explored the concept of separating out notions of data and device. An overarching goal of our approach has been to allow the *financially* valuable component of a device (i.e., the phone hardware) to be disconnected from the *personally* valuable component (i.e., the data it holds).

We have illustrated how the APPropriate approach is particularly beneficial in emergent user contexts where device security has been well documented as being a pressing issue [8, 14, 22]. This was particularly evident during evaluations in Kenya and South Africa, where many participants were worried about potential theft of their devices (Tables 1 and 2). Here, APPropriate was seen as a way to allow participants to leave their phone behind, but still have access to their data on-the-go.

Our studies also showed benefits of the approach for privacy, in particular when people share devices with others. Participants were more likely to be concerned about privacy if they shared their device with other people. Our results suggest that APPropriate is a potential response to issues around privacy on shared devices – participants saw the approach as a privacy-preserving way to store content created using shared devices, and potentially safer than using on-device hiding strategies [36].

In all of our studies, participants also saw benefits of APPropriate for sharing resources, both when consumables were exhausted (e.g., data, airtime, battery), and to take advantage of better features (e.g., camera, storage, screen). The general concept of separating out data and device is already prominent in mainstream computing thanks to the cloud computing revolution (e.g., synchronising documents between devices). In our view, however, this model is currently far from seamless when applied to the complete contents of a mobile device, and the APPropriate design hints at an alternative approach.

## LIMITATIONS AND FUTURE WORK

While APPropriate was fully functional, and usable on participants' own mobile devices, there are of course limitations of the work. We adapted an existing WiFi flash drive, rather than constructing custom hardware. Future versions could be sleeker in design, and able to be worn or hidden more discreetly. An option to directly connect to a phone via its dataport could increase synchronisation speed. Ideally, a version developed in collaboration with device manufacturers would also be able to be more deeply integrated into mobile devices from the outset. Doing so would both allow direct telephone networking functionality; and, permit fully-comprehensive content storage, perhaps by adopting similar techniques to existing cloud services, where all content is available, but full versions are retrieved only on-demand to reduce initial load time.

APPropriate was designed and co-created by and for emergent users. After undertaking this research we can envisage many areas of future work, both for emergent users and, more broadly, in other contexts. For example, mobile phone sharing is not currently the norm in many places. Were APPropriate-like systems to be widely available, they could stimulate and support device sharing, feature modularity; and, perhaps, technology non-use [3]. In this time of growing reaction to heads-down living [25, 34], we imagine people taking a break to disconnect from their mobile, safe in the knowledge that they could appropriate another device if absolutely necessary.

Finally, there are also clear areas of improvement to cloud-based account switching. However, the core contribution of this work is to encourage thinking more radically about solving these problems through *new* frameworks. We see our proposition as a research challenge in itself for others to take forward; as such we have made our prototype available as part of an open source toolkit.[5] The process of designing APPropriate, then, has helped focus a new lens on the fundamental design of mobile architectures, and also suggested potential directions for future mobile platforms for the rest of the world.

## ACKNOWLEDGEMENTS

This work was funded by EPSRC grants EP/M00421X/1 and EP/M022722/1. We thank Minah Radebe, Sharon Wangari, Francis Mwangi, Frankline Mogoi, Rini Ahirwar, Bhakti Bhikne, Nimish Maravi, Deepak Padhi and Anirudha Joshi.

[5]Toolkit available at: https://github.com/reshaping-the-future/pod

## REFERENCES


1. Jeremy Andrus, Christoffer Dall, Alexander Van't Hof, Oren Laadan and Jason Nieh (2011). Cells: a virtual mobile smartphone architecture. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles* (SOSP '11). ACM, New York, NY, USA, 173–187. DOI: 10.1145/2043556.2043574.
2. N. Asokan, Alexandra Dmitrienko, Marcin Nagy, Elena Reshetova, Ahmad-Reza Sadeghi, Thomas Schneider and Stanislaus Stelle (2013). Crowdshare: secure mobile resource sharing. In *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25–28, 2013. Proceedings*. Springer Berlin Heidelberg, Berlin, Heidelberg, Germany, 432–440. DOI: 10.1007/978-3-642-38980-1_27.
3. Eric P. S. Baumer, Jenna Burrell, Morgan G. Ames, Jed R. Brubaker and Paul Dourish (2015). On the importance and implications of studying technology non-use. *interactions* 22, 2, 52–56. DOI: 10.1145/2723667.
4. Stefan Berger, Rick Kjeldsen, Chandra Narayanaswami, Claudio Pinhanez, Mark Podlaseck and Mandayam Raghunath (2005). Using symbiotic displays to view sensitive information in public. In *Third IEEE International Conference on Pervasive Computing and Communications*, 139–148. DOI: 10.1109/PERCOM.2005.52.
5. Scott W Campbell (2007). A cross-cultural comparison of perceptions and uses of mobile telephony. *New Media & Society* 9, 2, 343–363. DOI: 10.1177/1461444807075016.
6. Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell and William Thies (2012). ''Yours is better!'': participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12). ACM, New York, NY, USA, 1321–1330. DOI: 10.1145/2207676.2208589.
7. Devanuj and Anirudha Joshi (2013). Technology adoption by 'emergent' users: the user-usage model. In *Proceedings of the 11th Asia Pacific Conference on Computer Human Interaction* (APCHI '13). ACM, New York, NY, USA, 28–38. DOI: 10.1145/2525194.2525209.
8. Jonathan Donner (2006). The social and economic implications of mobile telephony in Rwanda: an ownership/access typology. *Knowledge, Technology & Policy* 19, 2, 17–28. DOI: 10.1007/s12130-006-1021-7.
9. Chris Fullwood, Sally Quinn, Linda K. Kaye and Charlotte Redding (2017). My virtual friend: a qualitative analysis of the attitudes and experiences of smartphone users: implications for smartphone attachment. *Computers in Human Behavior* 75, 347–355. DOI: 10.1016/j.chb.2017.05.029.
10. James J Gibson (2014). The Ecological Approach to Visual Perception. Taylor & Francis. DOI: 10.4324/9781315740218.
11. Richard Harper and William Odom (2014). Trusting oneself: an anthropology of digital things and personal competence. In *Trust, Computing, and Society*. Cambridge University Press. https://www.cl.cam.ac.uk/~rja14/shb17/harperbc.pdf.
12. InFocus (2017). Kangaroo. https://www.infocus.com/kangaroo (visited on 12/09/2017).
13. Matt Jones, George Buchanan, Tzu-Chiang Cheng and Preeti Jain (2006). Changing the pace of search: supporting "background" information seeking. *Journal of the American Society for Information Science and Technology* 57, 6, 838–842. DOI: 10.1002/asi.20304.
14. Matt Jones, Simon Robinson, Jennifer Pearson, Manjiri Joshi, Dani Raju, Charity Chao Mbogo, Sharon Wangari, Anirudha Joshi, Edward Cutrell and Richard Harper (2017). Beyond "yesterday's tomorrow": future-focused mobile interaction design by and for emergent users. *Personal and Ubiquitous Computing* 21, 1, 157–171. DOI: 10.1007/s00779-016-0982-0.
15. Amy K. Karlson, A.J. Bernheim Brush and Stuart Schechter (2009). Can I borrow your phone?: understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '09). ACM, New York, NY, USA, 1647–1650. DOI: 10.1145/1518701.1518953.
16. Jennifer King (2012). ''How come I'm allowing strangers to go through my phone?"—smartphones and privacy expectations. In *Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM) at Symposium on Usable Privacy and Security (SOUPS) 2012*. http://www.jenking.net/mobile/jenking_smartphone_DRAFT.pdf.
17. Christian Kray, Patrick Olivier, Amy Weihong Guo, Pushpendra Singh, Hai Nam Ha and Phil Blythe (2007). Taming context: a key challenge in evaluating the usability of ubiquitous systems. In *Ubiquitous Systems Evaluation (USE '07), Workshop at Ubicomp 2007*. http://eprint.ncl.ac.uk/pub_details2.aspx?pub_id=159809.
18. Ramona Liberoff and Chris Horn (2011). Mobile identity and financial inclusion at the bottom of the pyramid. *innovations* 6, 4, 65–72. DOI: 10.1162/INOV_a_00101.
19. Siân E. Lindley, Catherine C. Marshall, Richard Banks, Abigail Sellen and Tim Regan (2013). Rethinking the web as a personal archive. In *Proceedings of the 22nd International Conference on World Wide Web* (WWW '13). ACM, New York, NY, USA, 749–760. DOI: 10.1145/2488388.2488454.
20. Yan Lu, Shipeng Li and Huifeng Shen (2011). Virtualized screen: a third element for cloud & mobile convergence. *IEEE MultiMedia* 18, 2, 4–11. DOI: 10.1109/MMUL.2011.33.

21. William Odom, Abi Sellen, Richard Harper and Eno Thereska (2012). Lost in translation: understanding the possession of digital things in the cloud. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '12*. ACM, New York, NY, USA, 781–790. DOI: 10.1145/2207676.2207789.

22. Fernando Paragas (2005). Being mobile with the mobile: cellular telephony and renegotiations of public transport as public sphere. In *Mobile Communications: Re-negotiation of the Social Sphere*. Springer London, London, 113–129. DOI: 10.1007/1-84628-248-9_8.

23. Jennifer Pearson, Simon Robinson, Matt Jones, Anirudha Joshi, Shashank Ahire, Deepak Sahoo and Sriram Subramanian (2017). Chameleon devices: investigating more secure and discreet mobile interactions via active camouflaging. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 5184–5196. DOI: 10.1145/3025453.3025482.

24. Thomas Reitmaier, Pierre Benz and Gary Marsden (2013). Designing and theorizing co-located interactions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13). ACM, New York, NY, USA, 381–390. DOI: 10.1145/2470654.2470709.

25. Simon Robinson, Gary Marsden and Matt Jones (2015). There's Not an App for That: Mobile User Experience Design for Life. Morgan Kaufmann.

26. Simon Robinson, Jennifer Pearson, Matt Jones, Anirudha Joshi and Shashank Ahire (2017). Better together: disaggregating mobile services for emergent users. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI '17). ACM, New York, NY, USA, 44:1–44:13. DOI: 10.1145/3098279.3098534.

27. Nithya Sambasivan, Nimmi Rangaswamy, Ed Cutrell and Bonnie Nardi (2009). Ubicomp4d: infrastructure and interaction for international development–the case of urban Indian slums. In *Proceedings of the 11th International Conference on Ubiquitous Computing* (UbiComp '09). ACM, New York, NY, USA, 155–164. DOI: 10.1145/1620545.1620570.

28. Nithya Sambasivan and Thomas Smyth (2010). The human infrastructure of ICTD. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development* (ICTD '10). ACM, New York, NY, USA, 40:1–40:9. DOI: 10.1145/2369220.2369258.

29. Alette Schoon (2016). Distributing hip-hop in a South African town: from the digital backyard studio to the translocal ghetto internet. In *Proceedings of the First African Conference on Human Computer Interaction. AfriCHI'16*. ACM, New York, NY, USA, 104–113. DOI: 10.1145/2998581.2998592.

30. Antero Taivalsaari and Kari Systä (2012). Cloudberry: an HTML5 cloud phone platform for mobile devices. *IEEE Software* 29, 4, 40–45. DOI: 10.1109/MS.2012.51.

31. Tails (2017). Live Operating System. https://tails.boum.org (visited on 03/01/2018).

32. James Tapper (2017). The moped menace: how the scooter became muggers' vehicle of choice. https://www.theguardian.com/uk-news/2017/jul/22/moped-menace-muggers-vehicle-of-choice-scooters-acid-attacks-phone-robberies (visited on 14/09/2017).

33. Alex S. Taylor and Richard Harper (2003). The gift of the gab?: a design oriented sociology of young people's use of mobiles. *Computer Supported Cooperative Work (CSCW)* 12, 3, 267–296. DOI: 10.1023/A:1025091532662.

34. Sherry Turkle (2011). Alone together: Why we expect more from technology and less from each other. Basic books.

35. Leena Ventä, Minna Isomursu, Aino Ahtinen and Shruti Ramiah (2008). ''My phone is a part of my soul'' – how people bond with their mobile phones. In *The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, 311–317. DOI: 10.1109/UBICOMM.2008.48.

36. Marion Walton, Gary Marsden, Silke Haßreiter and Sena Allen (2012). Degrees of sharing: proximate media sharing and messaging by young people in Khayelitsha. In *Proceedings of the 14th International Conference on Human-computer Interaction with Mobile Devices and Services* (MobileHCI '12). ACM, New York, NY, USA, 403–412. DOI: 10.1145/2371574.2371636.

37. Wikipedia (2017). Project Ara. https://en.wikipedia.org/wiki/Project_Ara (visited on 11/09/2017).