Imagined Connectivities: Synthesized Conceptions of Public Wi-Fi in Urban India

Nithya Sambasivan and Paul M. Aoki
Google Inc.
Mountain View, CA, USA
nithyasamba@google.com, aoki@acm.org

ABSTRACT

India and other economies in the Global South are undergoing a proliferation in public Wi-Fi, with large-scale deployments from industry and government. In this paper, we report on a qualitative study on public Wi-Fi conceptions as held by urban Indians, prior to connecting to a network. Our findings show that prior public Wi-Fi users and non-users alike raised a surprising range and depth of conceptions—ranging from suspicion of operators' intentions to monetize, to concerns about sexual image morphing, to fears of phone wipeouts, to aspiration—which were informed by popular media, Bluetooth cultures, and social learning. We found these conceptions of Wi-Fi networks to significantly influence adoption of public Wi-Fi. With enormous investments in public Wi-Fi initiatives, we call for network providers to address these deep conceptions among emerging users; by suggesting ways to build public awareness, better user experiences, and business model innovation.

ACM Classification Keywords

H.5.2. Information Interfaces and Presentation (e.g. HCI): User Interfaces

Author Keywords

ICTD, HCI4D, Internet, access, Public Wi-Fi, India, media studies, imaginaries

INTRODUCTION

India lags behind many other countries in terms of Internet access at an estimated 22% [53]. India's size, population, and emerging economy with stubbornly high poverty rates mean that truly ubiquitous deployment of high-speed infrastructure networks will not be economically sustainable any time soon.

In light of these realities, affordable public Wi-Fi is viewed as the democratic access solution for high-speed connectivity [44]. Accordingly, there have been several recent investments for large-scale public Wi-Fi deployments. For example, Google's partnership with Indian Railways and Railtel [52], Facebook's Express Wi-Fi [36], and Microsoft's TV whitespaces trials [34]. Similarly, the national government has committed to public Wi-Fi access for citizens through Digital India, the national infrastructure initiative that aims to connect 250,000 villages to optical fiber. Over 67 billion USD has been pledged for this initiative from companies within India alone [37]. India is not alone in this regard—public Wi-Fi is being deployed across the Global South, for example, México Connectado in Mexico [2] and DoST in the Philippines [19]. These public Wi-Fi initiatives remain free or low-cost in order to be accessible to a majority of people in emerging economies.

Communities in the Global South have been shown to seek out low cost or free-of-cost alternatives due to price-consciousness, lower affordability, and cultural norms. Users invest significant effort in improvising workarounds for low costs; examples of which include side-loading, piracy, and delayed access [51, 54, 66, 74]. However, in a qualitative study with middle-class urban Indians, we found that despite the economic incentive, even free and relatively higher speed service was not enough to motivate our participants to adopt public Wi-Fi. Many participants had tried and dismissed public Wi-Fi, or had refrained from trying it at all.

In contrast with the adoption pattern in the Global North, where Wi-Fi use became widespread before 3G/4G was widely affordable, all of our Indian participants already had access to mobile Internet (i.e., were *mobile-first* users [18]) before the introduction of public Wi-Fi. Public Wi-Fi was often perceived as superfluous in our study. Several participants would instead continue to use 2G/3G because it was "enough" for their needs. Some switched back to 2G/3G when they encountered poor experiences and negative conceptions of public Wi-Fi.

Despite Wi-Fi being in its nascent stages, participants in our study encountered public Wi-Fi with preconceptions from other sources, unlike earlier technological waves of the mobile phone or telecenters. The conceptions of public Wi-Fi connectivity drew not only on practical experience, Bluetooth cultures, and second-hand experiences but also, crucially, on meanings communicated through popular media. In common with anthropologist Arjun Appadurai's 'imagination as social

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s). Copyright is held by the author/owner(s).
CHI 2017, May 6-11, 2017, Denver, CO, USA.
ACM ISBN 978-1-4503-4655-9/17/05.
http://dx.doi.org/10.1145/3025453.3025545

practice' [1] [6], our participants invoked received notions of public Wi-Fi imaginaries from news media and popular culture. These conceptions were surprisingly rooted in real fears, deep insights, and specifics, whether firsthand or synthesized.

In this paper, we trace the user conceptions around free public Wi-Fi in India. We interviewed 2G/3G mobile Internet users who were occasional- or non- users of public Wi-Fi in Mumbai and Hyderabad. We found two factors that impeded connecting to public Wi-Fi.

- A complex depth of conceptions around unclear value propositions; fears of sexualization of identity, hacking of devices, incurring financial costs, and radiation risks of public Wi-Fi. Yet, there was an aspirational and 'modern' image of public Wi-Fi.
- Among those who had experienced public Wi-Fi, cumbersome and intrusive connection processes, regulatory requirements, and poor network qualities in practice led to frustration and abandonment of the networks.

We argue that public Wi-Fi initiatives should consider these conceptions while designing networks in order to influence adoption and uptake.

The research contributions of the paper are twofold. Our first contribution is a thematic description of these synthesized conceptions of public Wi-Fi, as assembled by participants from manifold sources. A second contribution is a set of suggestions for how public Wi-Fi providers and designers can cater to these conceptions through interaction designs and their associated business models.

This paper is organized as follows. We first describe the background of public Wi-Fi and our research approach. Next, we describe the Wi-Fi imaginaries, from the abstract aspirations to the specific threats. Then we describe the practical experiences of public Wi-Fi from prior experience and responses to our design provocations. Finally, we provide some suggestions for the design, policy, education, and business models around public Wi-Fi initiatives.

RELATED WORK

Prior research on public Wi-Fi

Scholarly research on the usage of public Wi-Fi is not yet extensive. From the literature on community wireless networks, there are a number of retrospective histories and experience reports (e.g., guifi [8]) as well as numerous traffic measurement studies (e.g., [3]). However, these studies provide only general information on user adoption and network usage. Our research focuses on the broader state of public Wi-Fi in India and specific conceptions that affect the trajectory of use or non-use of public Wi-Fi.

Qualitative user research of public Wi-Fi use in the USA and Europe (*e.g.*, Forlano on community Wi-Fi [28]; Hampton and Gupta on public Wi-Fi [31]; and Sanusi and Palen on coffee shop Wi-Fi [60]) frequently highlight two tensions. First, public Wi-Fi enables 'escape' from home or work. The escape is to a noisy, crowded 'third place' lacking physical privacy, but evades co-habitants/co-workers and their interruptions. Second, establishing clear legitimacy of users' claims to physical and non-physical hotspot resources [60] whether the network is free, paid, or an amenity for paying customers is often quite difficult for both users and venues. A general reluctance to pay for Wi-Fi [28] seems to motivate many to free-ride and take advantage of the fact that venue enforcement is often spotty and normative rather than technical. Qualitative user research in Cuba points to re-configurations in time and space planning due to the high costs of access [22]. The focus in these studies is generally on users who are motivated to take advantage of the infrastructure. In this paper, we extend these discussions by providing an account of how both Wi-Fi users and non-users make meaning out of public Wi-Fi, in a context where its penetration is nascent, but prior mobile data familiarity exists.

Security and privacy research documents a general lack of understanding of Wi-Fi and its security features, often leading to risky behaviors (*e.g.*, Kang *et al.* on Internet mental models [39] and Klasnja *et al.* on general Wi-Fi understanding among users [41]). Specifically, these studies show that Wi-Fi risks were ill-understood even in high-tech regions of USA, but practical details were well known. Less attention is paid to the choice of Wi-Fi non-use that might result from such misunderstandings; however, see [13]). In contrast to previous research in the west on user understanding, in our research, we find in-depth user conceptions of threats and poor experiences that led to a pause or reluctance to connect to public Wi-Fi.

We attend to the particularities of the Indian context, documenting TV, print, and social media around Wi-Fi; national policy; socio-cultural milieu; and infrastructural context. These conditions may apply elsewhere, for example, growing Wi-Fi, a healthy media, celebrity adulation, or government infrastructural efforts may give rise to versions of these conceptions.

Media and Wi-Fi

Media analysis has highlighted the incoherence of meaning associated with Wi-Fi by the public. Not only does Wi-Fi have multiple narratives favored by different stakeholders (e.g., 'openness and sharing' vs. 'security and convenience' [45]), but it continually acquires new meanings from other sources—every deployment site, implementing product, or monetization strategy comes with its marketing tropes and symbolic associations. One can relate these layers of meaning to Lefebvre's ideas on (schematic) representations of space and (symbolic) spaces of representation [33] and apply them to networks [21]. Here, we will limit ourselves to description, noting the connections drawn by participants between public meaning and their own views and behaviors.

[1] Our goal here is not to characterize imaginaries at societal scale, such as historical national identities (as in Anderson's imagined communities [5]) or sociotechnical futures. It is more in line with Appadurai's 'imagination as social practice' [6] and, in particular, his use of technoscapes and mediascapes to analyze individual agency within landscapes of technology diffusion and media narrative and imagery. Appadurai believes that global diffusion and new technologies have loosened the coherence of the Northern ideology in which these concepts were originally held together. Fact and fiction blur into each other. The scapes are disjunctive, deploying differently in each cultural setting, giving it different local meanings.

Internet access in the Global South

We briefly share the broader context of Internet access in order to situate the meaning of public Wi-Fi in emerging economies. Prepaid methods are used by a vast majority of mobile subscribers, as many as 95% in India [70]. Prepaid allows financial flexibility in top ups, made possible by ubiquitous top-up shops. Internet access is generally characterized by slow speeds and high costs (as a proportion of income) [35]. Internet usage is, therefore, rationed and deliberate [18, 59, 74], with a 'metered mindset' [18] and a range of strategies to keep costs low [49, 59]. Low-cost and low-end smart phones, primarily on Android OS, are on the rise [23], although gifting, sharing, second-hand phones, and hand-me-downs are common [54]. Public Wi-Fi co-exists with this constrained space, providing higher speeds at lower costs.

THE LANDSCAPE OF PUBLIC WI-FI

Basics of public Wi-Fi

By public Wi-Fi we mean Wi-Fi access networks intended to serve users in public places. We do not assume that public Wi-Fi networks are public in the sense of being owned by the public (e.g., a municipal government), operated by the public (e.g., community Wi-Fi), openly accessible to the general public (e.g., unsecured), or free-of-charge to the public—though they may be any of these.

From a global network design perspective, Wi-Fi spectrum is usually unlicensed and can therefore be very cost-effective.

There are a number of common payment models for public Wi-Fi. Access may be free-of-charge, offered as an amenity or with ads. Access may be billed to the user's mobile data or charged directly. Similarly, there are several ways to access public Wi-Fi [27]. Most common is the captive portal, in which the user enters information into a web page to get access. Some venues, especially smaller ones, offer unsecured or pre-shared-key-secured networks (PSK). And a few venues offer carrier Wi-Fi, where mobile network credentials are used to authenticate the customer and bill their mobile data.

Public Wi-Fi in India

The rising number of smartphones, ease of deployment of Wi-Fi, and low fixed line penetration motivate telecom and government alike to provide high-speed connectivity in public locations [44]. India appears to be at the cusp of public Wi-Fi growth with massive investments from industry and government. Unlike the west, community or municipal Wi-Fi has not taken off in India and public Wi-Fi remains a venue-based service [44].

All public Internet access in India, including hotspots and cybercafés, are required to follow the Know Your Customer (KYC) protocol of identity verification after the 2008 Mumbai terror attacks [38]. Captive portals are commonly used for KYC login by big venues. Mobile phone numbers are 'traded' for a verification code to confirm the identity of the device/user, which is used to login to the network. Due to its cumbersome steps, detrimental effects on user experience, and panopticon-like enforcement of revealing personal identities, the KYC process has met with dissent in India [62].

A note on the Indian technological context is imperative. As of 2016, India has a population of 1.28 billion, out of which 306 million use mobile Internet [1]. 2G is the dominant network due to coverage and affordability. GSMA expects 50% of Indian subscribers to stay on 2G even in the year 2020 [61]. In an Ericson survey, 88% of respondents felt 3G was too expensive [23]. Only 19.8 million households have access to fixed-line broadband [70]. Public Wi-Fi, while growing, is still in the early stages at an estimated 31,000 hotspots nation-wide [44].

METHODOLOGY

Participants

Semi-structured interviews were conducted in the cities of Hyderabad and Mumbai, India during July-September 2015 for a design ethnography project [56] intended to inform a public Wi-Fi initiative. Participants were recruited through an external recruitment firm, to which screening criteria were provided. We interviewed thirty-six people altogether, eighteen men and eighteen women. Participants were recruited across a diverse range of ages (19-64), low- to middle-income socioeconomic groups, and occupations including college students, homemakers, working professionals, retirees, service workers and unemployed people. As the research was intended to inform a new, access-broadening Wi-Fi initiative, the focus was on nascent users, although public Wi-Fi itself is recent in India. All participants owned a mobile phone—typically a low-end Android smart phone, though a few owned feature-phones—and all had access to prepaid mobile data, though most used the data intermittently. Nine participants had access to fixed-line or mobile broadband Internet in the home as well. Most (26) had no prior experience with public Wi-Fi and the rest (10) had used public Wi-Fi at least once; 16 had prior first-hand experience with Wi-Fi at home or work.

Method and analysis

Interviews lasted two hours each. Interviews were conducted in Hindi, Telugu, and English. Interviews were conducted by the first author; the second author partnered on analysis and synthesis. No personally identifying details were collected. All data were transcribed securely online. Pseudonyms are used when discussing participants below.

The interviews were conversational in style, but covered a fixed set of questions around Internet and Wi-Fi use. Questions focused on the awareness, discovery and attitudes around Wi-Fi; device and app use; behaviors on Wi-Fi networks including non-public Wi-Fi networks; contextual factors in venues; and pain points on networks located in venues. After the in-depth interviews, low-fidelity design provocations for captive portals were shown for feedback. The design included a simple multi-step login process following KYC, abstracted from currents models of captive portals (described later in the 'practical experiences' section; see Figure 3). The provocations were printed on paper to remove technological intimidation and to create room for comfort and scribbles. Questions around the provocations were centered on value, attitudes and perceptions around the wireless technologies and the connection process. The goal was not to evaluate the usability of the design, but

to shed light on prior connection experiences and high-level architecture of the design components.

Interview data were analyzed using a general inductive approach [68]. Our evaluation objective was to elicit factors to inform the design of public Wi-Fi systems. Next, transcripts were read multiple times, affinity clusters were developed, and key themes were derived and iteratively refined. Forty-four codes were developed, for example, security and place-based behaviours, which were developed into themes discussed here. We focused on characterizing the experiences and understandings of public Wi-Fi.

Sites

Hyderabad and Mumbai were chosen as the sites of study, to understand public access in metro cities of two sizes. Mumbai, state capital of Maharashtra is the financial capital of India with a population of 18m. Ethnically diverse, Mumbai has global wealth and local poverty at once [7], with a vibrant commercial culture, including banking and Bollywood, and a thriving shadow economy [54]. Hyderabad, state capital of Andhra Pradesh and Telengana, is home to pharmaceutical and technology companies, including Google and Microsoft development offices. The city is more traditional in lifestyle and cultural attitudes than Mumbai.

WI-FI IMAGINARIES

Technologies are envisioned, translated, resisted or consumed in relation to their socio-cultural contexts. In our study, the imaginaries of public Wi-Fi as held by participants drew from an assortment of local news media, national policy, popular culture, carryover notions from prior technologies like Bluetooth, and personal experiences. Public Wi-Fi, then, goes from an invisible connectivity technology to a material medium with pre-existing values, anxieties, expectations, and experience attributes. Similar to Dourish, we approach public Internet in light of its social and cultural effects, but also maintaining a focus on its material realities [20].

In this section, we present the various imaginaries of public Wi-Fi as held by participants in our study. As such, each person spoke of several different conceptions of Wi-Fi. The multilineal conceptions co-existed with each other. Many of these motivated them to try Wi-Fi, whereas others were discouraging. Taken together, they forged a more calculated, speculative, and hesitant experience with public Wi-Fi. First, we illustrate the aspirational aspects of public connectivity circulated by media and welfare policies. The introduction of Wi-Fi as part of civic life invoked images of modernity, national development, pride, and social connectedness among our participants. These positive conceptions were relatively abstract frames for the desire to connect to public Wi-Fi.

Next, we highlight the conceptions around fears and concerns. In contrast with the abstract positive conceptions, these conceptions related to direct and specific threats: privacy and personal safety, security, personal health, financial implications. The threats were derived from scientific, biological, sociological, financial and experiential sources. Like positive conceptions, these conceptions drew extensively on media reports and public discourse as well; but personal experiences were understood in light of such information, making them seem more damaging to real life. While several of these conceptions may be found worldwide, the magnitude, legitimacy and consequences of these fears are much more nuanced and severe in the Indian context, which we elaborate later.

Development, modernity, and 'fashion'

Public Wi-Fi imaginaries were painted with broad strokes of socio-economic development, modernity, and trendiness by national policy and media. First, the discourse of the grand national infrastructure projects had a remarkable influence on awareness and imagination around Wi-Fi in our study. The Digital India campaign produces high visibility announcements, state visits, and public-private partnership launches that are widely covered in news media [55]. The Indian Prime Minister, titled 'India's first cyber premier', colors citizens' technology perceptions with his pro-technology stance and regular use of social media [50]. At the state level, provision of public Wi-Fi is often a part of electoral manifestos, modeled on programs in global cities such as Shanghai and Singapore [26]. The rollout of public Wi-Fi is viewed as a part of the continuum of India's technological emergence; depicted by media as placing the country on the 'information superhighway' [69].

In our interviews, participants, including non-users, were highly aware of public Wi-Fi initiatives in their cities. Public Wi-Fi was broadly viewed as a public amenity for the welfare of tax-paying citizens, a program for national and urban development, not just as venue-based services. All participants knew from media reports of locations where it was being set up, including parks, public squares and private establishments. However, Wi-Fi availability was not predictable in public places due to its early stages.

Our participants often described Wi-Fi, particularly in the public sphere, as 'fashion,' a term signifying its trendy and modern associations. The Internet has long been a signifier of modernity and progress. Larkin notes that infrastructure does not just operate on the technical level, but also on the level of fantasy and desire [43]. In our interviews, the convenience of accessing Internet and being connected to any part of the world was described as 'modern'. The spatial and situated nature of access from places where participants wanted to be seen in, such as Starbucks, Café Coffee Day or InOrbit Malls, made the Wi-Fi more coveted and turned it into social currency. In more mundane places like bus stops and train stations, the presence of Wi-Fi was viewed as a positive delight, "elevating the experience". Even with mobile data being available in most places, Wi-Fi as an amenity for customers or citizens was seen as exclusive. The material aspects of public Wi-Fi presented it as an icon of status and modernity in the public spaces, similar to Spitulnik's observation of radio sets in Zambia [67]. Nisha, 27, a beautician, observed how high speed Wi-Fi invokes pride, and how the national capital enjoys more benefits:

"It's fashion. College students and teens like to use Wi-Fi in our age group. The students and youth want to share their pics and their feelings immediately. If Wi-Fi is faster than mobile data, you can be proud of using it, you can tell your friends you are using Wi-Fi. In Delhi they have a road. They did a study on it, I saw on Google called 'Wi-Fi Road' or something.

We also should have it, not like Necklace Road, where the speed is pathetic. Hyderabad should become modern."

Second, independently of government announcements, the media carry a thriving discourse on technologies in India. Kavoori and Chaddha argue that the process of appropriation of technologies in the Global South occurs not through Internet media, but through mass media like televisions, newspapers, and magazines [40]. Front-page and full-page newspaper ads for the latest gadgets are commonly found in India. Physical marketing collateral, like billboards and posters, for technologies can be found in most urban and some rural areas. Indeed, twenty one participants described wide media coverage as the first test of credibility.

Third, another influencer of public awareness of technology was the film industry. Popular films exert an enormous influence on public culture, politics, ideologies and lifestyles in India [16]. Unsurprisingly, the advertising industry leverages the public adulation and goodwill vested in film celebrities to sell products. Not only are celebrities brand ambassadors for popular products; less well-known and upcoming brands are also endorsed by them to increase brand value (see an account of how the public image of a celebrity actor affected app installs [25]). Sapna, 41, a homemaker, connected film actors with public honesty:

"It would be better if a hero I admire like Amitabh [Bachchan], or someone my daughter admires, like Varun Dhawan, did an ad for new Wi-Fi in the city. They will not lie to us."

Finally, word-of-mouth played a huge role in diffusion of new technologies. Social intermediation for first-time Wi-Fi users from their friends and family had helped them navigate the connection process and get on the network for the first time [58]. Word-of-mouth and credibility through social networks were also noted to be factors in trying out new services. Harish, 35, a factory supervisor noted:

"I will wait until other people use Wi-Fi and give reviews. I really trust my friends and family members. If they confirm it's good, then I try it. They tell me where it's free and good."

To sum up, public Wi-Fi was portrayed and perceived as nation-building infrastructure, social currency, and a vision of global modernity. Yet, specific fears often trumped these aspirations and desires, moving and shaping reluctance with public Wi-Fi. We now turn to a description of these perceived risks.

Sexualization and spam

Public Internet access in India must be understood in the context of a few social themes relating to privacy. For domestic security, all public Internet providers must follow the KYC protocols (see above). Implementations of KYC results in two main concerns, often rooted in experience. First, that personal information is not well protected by those who collect it. Second, sexual harassment of women, wide reporting of harassment and sexual violence cases (*e.g.*, [65]) that resulted from simply appearing in the public sphere, gave female participants pause about revealing any identifying or personal information to strangers. In this section, we describe the various personal information fears expressed by our participants as they relate to public Wi-Fi login and usage.

Participants reported experiences with Wi-Fi access provided through captive portals, password-secured networks, and unsecured networks. Recall that in India, mobile phone numbers are required in the online registration process, with one-time passwords sent via SMS to confirm the validity of the collected number. However, in our study, three of the Wi-Fi users reported logging in to unsecured venue-based networks, which presumably violates regulatory requirements. The obvious user experience issues and the need to deploy software infrastructure for captive portals may motivate venues to provide simpler password-secured and unsecured networks. Due to the slow login process with OTPs, sometimes as long as 10 minutes, ten participants reported often logging in to a better experience with unsecured networks.

In giving out the phone number for login, participants reported being spammed with marketing messages and apparent selling of personal information to telemarketers. These experiences did not instill confidence in captive portals. In addition to requiring mobile number entry for verification, several captive portals presented additional fields for personal information, such as full name, e-mail address and home address. Even though these fields were marked as optional, most participants in our study did not pay attention to the optional tag; instead, they reported feeling uncomfortable and intruded upon. Thirteen participants had enabled 'Do Not Disturb' (DND), a service to block unsolicited SMS that is widely used in large cities [64]. Others, more ambivalent about marketing, did not. Ram, 41, a manufacturing executive says:

"AP [Andhra Pradesh state] government introduced Wi-Fi in public places like trains, but it takes so much time. They are asking for your number, only if you give your number then they give you the password. It was taking 30 minutes to get the OTP. Then they will sell the data to marketing companies. But I have not enabled DND because sometimes I get calls or coupons, like they asked me and my wife to come and collect a gift. We didn't go. If a place asks for a password, you just leave it. Never put a phone number."

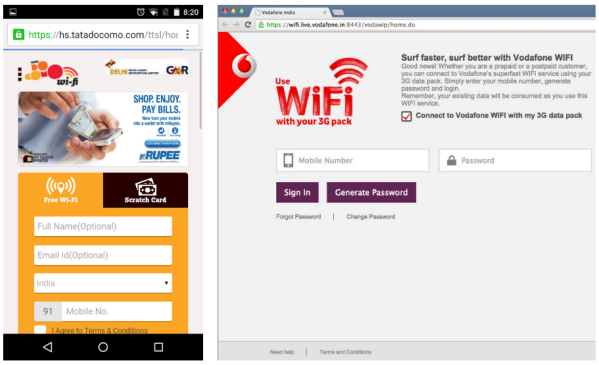

Figure 1. Sample captive portals mentioned in the study.

While provision of personal information caused discomfort for most, this was particularly acute among women. Fears included using phone numbers for prank calls, using personal

information for stalking, and morphing profile photos into pornographic content, a reputational attack that occurs in other regions as well [14]. While public sexual harassment is a worldwide problem (see [17]), it is much more visible in the public sphere in India since the gruesome 2012 Nirbaya rape incident [65]. For example, rape assaults are regularly covered by national news media. In turn, the public discourse around harassment may have led to a more pronounced consciousness around personal safety.

In particular, captive portals seeking personal information such as phone numbers, full name, or zip code were considered intrusive by female participants among both Wi-Fi users and non-users. Incidents of personal information misuse and its devastating consequences on women led to a recognition of the side effects of data trails online. Online fears are tied to offline consequences, such as physical stalking and groping, in South Asia [4]. As an example, a 21-year old female committed suicide after her Facebook profile picture was morphed into a nude image [24]. A less damaging experience mentioned by eight participants was being stalked online or receiving friendship requests from strangers.

Although technically captive portals cannot abuse profile pictures, such fears were profound among female participants and seven even reported abandoning Wi-Fi logins to avoid entering their phone number. Five female participants reported sharing only their secondary or tertiary SIM numbers or their spouse's phone number for public services. Anu, 34, homemaker, says:

"I don't like if they ask me for my number when connecting. They can misuse. We are ladies, we face more harassment problems. You are always thinking: will they send us a message like a dirty message? Or take our profile pic? Women only give details to people they know. If the person asking is a good person I will give, but how do I know? I'll give other people but I won't give to Wi-Fi. Why do they need name, phone number, address and all these personal details? What are they going to do?"

While the collection of identifying information no doubt seems prudent to officials concerned with domestic security, a widespread concern that unknown parties will abuse this data can be seen in non-use patterns in our study.

My 2G is good enough

Since the vast majority of India does not have access to a high-speed connection, public Wi-Fi is a preferred route for broadband networks in India [44]. Despite its purported higher speeds and relatively low costs, public Wi-Fi did not always offer clear benefits in comparison to mobile data or home broadband to our participants. In this section, we highlight how existing mobile data connectivity felt superior to public Wi-Fi to many participants in our study.

Wi-Fi was generally associated with "free," "fast," and "reliable", imagined as the fastest technology, followed by 3G and 2G. Still, 2G was seen as adequate for Internet needs. Similarly, in spite of the general association between Wi-Fi and "free," i.e., being cheaper than mobile data, cost savings were described as a minor motivating factor in trying public Wi-Fi. Instead, participants portrayed surprisingly complex reasons for whatever interest they had in public Wi-Fi.

Nine non-users of Wi-Fi stated a preference to use their 2G data plans instead of hotspots. There are many reasons for this. High speeds were seen as more relevant for IT professionals and tech-savvy users. Sambasivan *et al.* [57] report a similar observation for wired networks. While 2G mobile data provided limited speeds, popular lightweight limited activities, such as social media, were seen as acceptable on the networks. High-bandwidth activities, such as streaming and gaming, had limited occurrence or achieved through side-loaded means. Public Wi-Fi was not associated with enrichment, convenience, or high-quality experiences, unlike in other contexts where Wi-Fi is used in public venues.

Here, Kiran, a 36-year-old secretary who did basic tasks online explains her hesitation to try free public Wi-Fi. Note Kiran's comfort with terms like 'MBs' and '2G net pack,' data plan concepts that were familiar and regularly used by other participants as well:

Kiran: *"I don't know what is this Wi-Fi. My children and neighbors talk about it, but I don't know much. I already have MBs from my 2G net pack, so why would I use it? They are not going to give my MBs back. I have 2G. It works for me. Even if it is free, I will not use W-Fi."*

Kiran characterized her net pack purchase as a sunk cost and did not see how using free Wi-Fi would benefit her. Given the cost-consciousness in this context [49], the hesitation to connect to a network at no or low cost is surprising.

Viruses and wipeouts

Being connected to a public, shared network led to an acute sense of vulnerability in our study. Hacking, receiving or sending malicious content, and phone wipeouts were consistently brought up as concerns when connecting to public Wi-Fi, issues not generally raised in western world studies (*e.g.*, [39, 41]). In this section, we describe the various conceptions as they relate to the 'public' nature of public Wi-Fi networks.

Concerns of hacking were focused on device hacking and content deletion, rather than misappropriation of account information, unauthorized transactions or sharing private data; in terms of Wash's folk model of viruses, "mischievous" rather than "criminal" [72] (which contrasts with most other findings, *e.g.*, [12, 41]).

In many cases, concerns appeared to be a form of transfer learning from more familiar wireless networks—notably Bluetooth—to Wi-Fi. Bluetooth was adopted for sharing and side-loading of previously downloaded media content (*e.g.*, movie songs and photos) in the days of feature phones. Wireless sharing with friends, family and bare acquaintances has become widespread social practice [66]. By downloading and side-loading content through multiple hops, media and file content are prone to virus infections. Six participants narrated personal experiences and anecdotal stories of getting viruses from sharing offline content, leading to slowing down of phones or resetting the OS (although these instances could result from low-end phones with overloaded RAM crashing,

similar to [66]). With causality of phone wipeouts being difficult to point to, there was general anxiety and caution with connecting to public networks, from carryover fears. Yamuna, 28, reported how her entire phone was wiped out, including beloved selfies, a large contact list and carefully curated song collection, just after receiving a song from her neighbor on Bluetooth. She then took her phone to a repair shop to restore and set up, now with anti-virus software. Any network with sharing, according to her, then became insecure; Yamuna refused to connect to any public Wi-Fi network because she wanted "no chance of risking my phone again."

While the security concerns brought anxiety to Wi-Fi users, they did not always prevent them from connecting wirelessly. Seven prior Wi-Fi users expressed "many people are connected", concerned that networks could be vulnerable to strangers reading their data bits. In some cases, the relationship between wireless networks may not have been clear, let alone which networks were more likely to spread infected content. Bhanu, 35, a lawyer narrates:

"Trust factor is very low. My husband connected to the Wi-Fi at CCD and he got some requests because the Bluetooth was on and he was connected to the network. He transferred a few songs and a movie and he got a virus. He had to reformat his phone. It was too much. My friend had to reformat her laptop. She blames the Wi-Fi for getting the virus. So many of my friends tell me not to use public Wi-Fi."

Low personal awareness of technology and its consequences was also cited as a reason to not use public Wi-Fi. The perspective here was to avoid a new technology because of too many security unknowns. Vaibhav, 44, a corporate trainer narrated:

"I have a friend that refuses to use Wi-Fi, he still uses the wires. I think, 'This is a smart guy, and I am a stupid fool. I think he knows something. Am I going too far with this technology?' So many hackers are there. Who knows if my phone will get hacked if I use Wi-Fi?"

Other concerns raised around seamlessness were control over network selection, owner of the data brands or networks and personal information misuse (see above).

As an illustrative aside, Wi-Fi in the home was viewed as very different from public Wi-Fi due to the ability to set private network passwords, analogous to [12, 39]. The ability to assign one's own password, as opposed to one generated by a source of limited trust, or being authenticated by strangers running a captive portal enabled a feeling of control over the network. Mobile Internet was also viewed as a secure connection. Four users viewed public networks with KYC logins and PSK passwords were viewed as more secure (recall that some venues provide unsecured Internet access without captive portals or passwords).

The participants' conceptions of Wi-Fi intermixed public discourse on online safety (hackers attacking wireless networks, strength of passwords) with personal experience (prevalence of viruses), confusions (conceiving of Wi-Fi as more risky than other types of networks) and social norms (expectations of response to sharing requests).

Personal health

Health concerns from Wi-Fi emissions were seriously regarded in our study. Electromagnetic fields (EMF) from mobile networks and devices receive regular press and government attention around the world [73]. In our study, radiation risks regularly surfaced in TV, news and social media, leading to limited use or apprehensions about using public Wi-Fi.

Seven participants in Hyderabad mentioned viewing a recent television news feature on Wi-Fi health risks. The program discussed the radiation risks of using Wi-Fi with scientific-sounding facts and real-world examples of corporeal damage through cancer, brain damage or animal and bird deaths. Ahmed, the nutritionist was one of the viewers of the program. Here he talks about the credibility of a feature on national television; since viewing the program, he switched off his phone at nights and avoided using Wi-Fi in public places. In Ahmed's view, using the Wi-Fi was a "dose of radiation, you use very less or don't use at all."

"Wi-Fi causes health problems. I have seen it on TV, NDTV or Aaj Tak. They did a special show on Wi-Fi. My daughters and I got very scared. We shut off our Wi-Fi for two days. It can cause mental disorder or cancer. They showed that sparrows can die. It was on national television, so they can't fake it. They advised us to shut off the Wi-Fi router when we are not using it. In public places we can't shut it so I avoid completely. If you keep any mobile in your pocket with Wi-Fi, you will feel the rhythm of your heartbeat changing."

Ahmed was one of the few participants who avoided public Wi-Fi due to health concerns. Seven prior users expressed worries about Wi-Fi radiation and self-capped their usage.

Social sharing of news items through WhatsApp, Facebook and regional magazines reinforced these messages. Often these messages carried weighty qualifiers, such as international news, health or astronomy organizations; severe health risks that cannot be dismissed easily; and emotional significance in sharing the health warnings to close ones. Burrell, in a study of rumors in Ghana, notes that they at once combine vague animosity or threats, attached to concrete events and times and institutional responsibility [11]. Chitra, a 35-year old banker, showed us a recent forward on NASA- and BBC-approved phone radiation warnings she received (which has circulated since 2010 in Ghana and been declared a hoax (see Figure 2) [9]). She forwarded the message to three of her relatives. Public Wi-Fi to Chitra was part of a larger class of radiation prone technologies, indistinguishable from mobile phones.

The risks of Wi-Fi were perceived not only in public Wi-Fi networks, but also in home networks; in fact, five participants unplugged routers at home, motivated by frugality as well as health reasons (also noted in [57]). As Swapna, 39, a homemaker, reflected on the inadvertent connection of her phone to her neighbor's Wi-Fi, even when she unplugged her router. Eventually she switched off her phone Wi-Fi toggle:

"Wi-Fi can give you headaches... At night we switch off the Wi-Fi network in the home. But our tenants live downstairs in 50m radius. Sometimes my phone connects to their Wi-Fi at night. Then we told them to switch it off. After 11, no Wi-Fi."

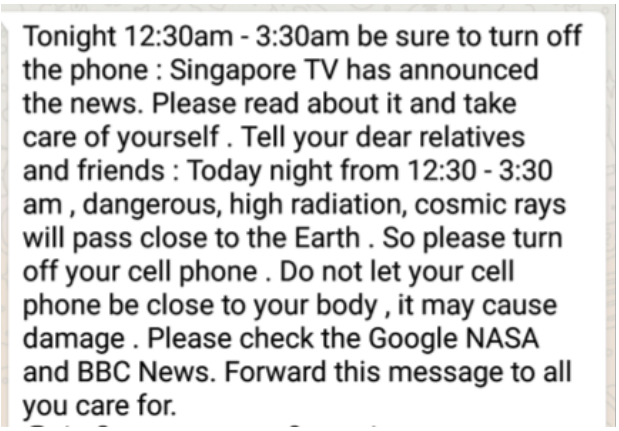

Figure 2. A Whatsapp forward received by a participant.

In their concern about EMF, these participants are no different from any number of concerned citizens worldwide; cancer fears concern British elders [42] and cause Kenyan and Zambian farmers to switch off their phones [73] as well. What is notable here is the attribution of physical effects, real or not, to EMF from Wi-Fi but not from mobile networks and the focused discourse on the risks at national and social levels. For example, neither informant speaks of 2G handset emissions, which are at much higher peak power levels [71]. Indeed, notice that the way that Swapna detects her tenants' Wi-Fi is by the fact that her smartphone connects to it.

It is the "new" technology that is singled out in public discourse of news and social media, in personal concerns (fear), in corporeal sensitivity and in concrete response (non-use). As in earlier responses to mobile towers (*e.g.,* [10]), the focus is not on fully removing the infrastructure in use, but on the *control* of infrastructure coming into use. As in ubicomp research on off-the-grid "disconnectors", disconnection from infrastructure is selective rather than total and irreversible [46].

Financial fears

News stories, government announcements, and commercial advertisements had created an expectation among all participants that free-of-charge use was the norm for public Wi-Fi. When asked if they had ever paid for Wi-Fi access, participants resoundingly replied in the negative: "*Never! If you have to pay then why do I have mobile data?*" Given this, it may seem strange to characterize cost as a specific threat of public Wi-Fi.

As is often noted in studies in developing regions, a key issue for prepaid telecom users is direct control over costs [49, 59]. Acquisition of prepaid data packs involves meticulous planning around the amount of data, validity, and cost. Lack of clarity around how usage is billed in public Wi-Fi threatens users' control over meeting their communication needs under a constrained telecom budget. Non-users expressed suspicions that Wi-Fi advertised as "free" would turn out to cost something after all. Here the distinct entities of time on Wi-Fi networks and mobile networks were viewed as fungible, boundary-less monetary units. Two non-users expressed that free-of-cost usage still did not clearly indicate to them whether their mobile data balance would be cut off.

Confidence had been established in their operators' billing rates and practices given their current usage. It was not a small thing to abandon the familiar data pack for an unknown entity (public Wi-Fi operators), even one that promised free use and potential for high-speed use cases.

PRACTICAL EXPERIENCES OF PUBLIC WI-FI

Up to this point, we have mainly discussed the conceptions held by participants about public Wi-Fi that steered them toward or away from adoption, or at least experimentation. We now turn to the practical experience of accessing public Wi-Fi. We summarize participants' responses to our design provocations and recollections of prior experiences with captive portals (see Figure 3). Note that in order to be displayed, captive portals require a user to open any http URL on a browser or open a phone notification.

Confusion with captive portals

Participants found captive portals to be confusing and error-prone; connecting was not an obvious process. First, twenty-one participants, including public Wi-Fi non-users and even a few self-identified users mentioned that upon connecting to an unsecured network, they would go straight to application use. That is, the intermediate step of opening the captive portal page to sign in did not fall within the natural course of expected actions. Fifteen participants expressed that unsecured networks need no further step. In practice, the individual would not be connected to the network.

Second, in walking through the captive portal process, there were drop-offs. The KYC process was not clearly understood, hence these individuals did not expect to receive or check SMS. Twelve participants, especially women, expressed privacy issues of refusal to enter phone numbers and other personal information (see above). A common touchpoint for determining whether one was finally online was when social media messages started flowing into applications. Five participants forgot their access code from SMS by the time they toggled to the browser. Of these, three wondered if they should send a reply to the SMS received. Prior Wi-Fi users had a clearer understanding of the KYC captive portal process that non-users; but not uniformly since some had connected to open networks or PSK-protected networks (see above).

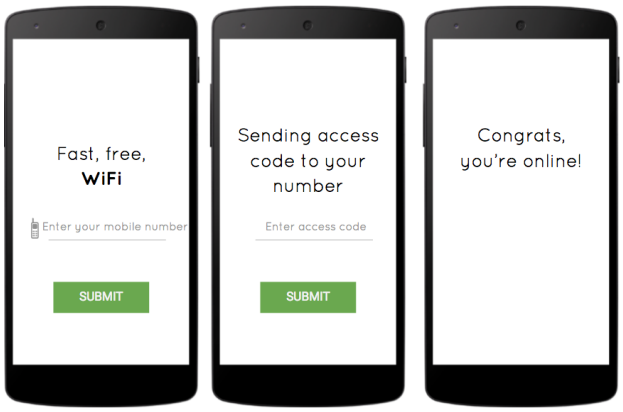

Figure 3. Design provocations used in the study.

Slow speeds

As mentioned above, Wi-Fi as a concept was associated with "free, fast, and reliable," but in public places it was considered slow by those who had actually used it (in practice, poorly provisioned Wi-Fi can be as slow as 2G). Not only was the actual connection reported to be slow, but the KYC login on captive portals was also reported to take a while. Six participants reported abandoning the connection process when they did not receive an access code in a few seconds.

Due to the unpredictability of availability at a future locale, of actual speeds, and so on, public Wi-Fi was never the go-to network for doing things online in our study. Rather, it was used for low-priority browsing. Mobile data, even 2G, was viewed as a lot more dependable. Fourteen prior Wi-Fi users connected to public Wi-Fi to find an alternative when mobile data was exhausted or running low. On low balance, their intent to connect surfaced not because a Wi-Fi network was available and one was habituated to a continuous connection, but because an activity arose that required online access.

Discovery of Wi-Fi

The process of getting connected to a public Wi-Fi network was involved and resource-intensive. Notification alerts for local Wi-Fi networks did not appear for most, as a majority (twenty-six) of our participants (even prior users) kept their phone Wi-Fi turned off. Eight of those with home Wi-Fi also turned off Wi-Fi when outside. This mirrored the widespread practice of turning off mobile data to save battery power and prevent background data usage by applications [49]. Instead, discovery of public networks was accomplished through physical posters and word-of-mouth.

Discovery was characterized by gendered concerns. Studies have documented gender gaps in phone access in South Asia (women are 38% less likely to own phones in India) [30]. Six female participants wanted to run new technology by their spouses for approval. Among them, technology adoption decisions were deferred to men. Three female participants expressed concerns about being intimidated by seeking help from male staff, the social consequences of conversing with males, and mis-trusting strangers. Ameya, 29, a tailor, reflects:

"I would come home and talk about Wi-Fi, if I see it. My husband would ask me, 'why did you talk to someone [the agent], why do you trust this person'. He says people do make a fool out of wives, but not husbands."

DISCUSSION

Based on the experiences of participants in our study, we note that public Wi-Fi is approached with a complex set of imaginaries, from multiple sources. In the words of Malinowski, '*myths are not merely stories told, but realities lived...myth, is not merely symbolic, but a direct expression of subject matter*' [47]. Despite the aspirational leanings, the conceptions largely encompassed deep-rooted fears and risks, impacting the adoption and usage of public Wi-Fi.

How does a new technology co-exist or conflict with the social practices and material properties of existing technologies? Infrastructure studies underscore that infrastructures are formed when several technological systems combine to form a union: light bulbs succeeded not due to the mere innovation in bulb design, but from linking many underlying financial, technical and administrative systems [43, 32]. As a recent network technology, public Wi-Fi was surrounded by hype in national development, urban modernity, and media advertisements. Yet, points of friction from previous technology cultures surfaced in phone wipeouts fears, or when relevancy of Wi-Fi seemed low compared to 2G. With a fallback option of 2G, many participants did not want to make the effort to switch, or converted back when fears or frustrations with Wi-Fi arose.

While a public hotspot can be set up by any establishment by lighting up an access point, our research points to a non-trivial number of aspects to get right for adoption. If the network is not well provisioned; the login process difficult; the value of using public Wi-Fi over mobile data unclear; or the fears and concerns unaddressed; public Wi-Fi may not feel inviting to many. However, these factors are not insurmountable and successes are starting to emerge. The recent deployment of Wi-Fi in train stations by the Google partnership with Indian Railways and RailTel had 5 million users as of Dec 2016 by providing a spam-free, high-speed, simple login experience with several branding touch points [48].

With the data above in mind, we can now develop some general points relevant to the idea of Internet ubiquity in India.

Public Wi-Fi as approachable networks

We can expect that public Wi-Fi access will continue to expand, due to government and industry interest in providing infrastructure to the public. The contours of Wi-Fi continue to shift, as it evolves as a technology and more people encounter it in India. As an infrastructure gains prevalence and prominence over time, fears and concerns may diminish or transform [10].

If public Wi-Fi were to be truly democratic, the design of these infrastructures need to consider less resourced individuals who may get marginalized due to the embedded politics [43]. Designing experiences that do not reinforce existing socio-economic privelages, such as literacy, gender, affordability, or social class, by making the experiences safe, intuitive, low cost and inclusive. Experience providers should clearly state cost implications of connections, to avoid user confusion about using up mobile credit or bank balances. Since open networks were associated with compromised security, any measures of security from captive portals are paramount. Health concerns around radiation risks or eye problems from using Wi-Fi networks could be clarified through legitimate TV shows, radio programs or social media forwards from carriers.

At the same time, awareness initiatives around the connection itself may help make systems more usable, draw relevance and remove fears around Wi-Fi. Guided walkthroughs on user devices may make the networks seem more relatable and help users assess the quality firsthand. Human agents and kiosks are widely employed in India and other emerging economies to introduce new concepts and were considered easily approachable in our study [66].

Public Wi-Fi as infrastructure for the public

Public Wi-Fi operates in public space and was imagined much like a public space: locational, shared, and subject to overuse, unlike mobile networks that were perceived as pervasive, private, and consistent. The shared network often created a feeling of vulnerability. Many KYC implementations requested more information than needed. Intrusive implementations of KYC led to concerns about personal identity misuse and sexual harassment, leading to refusal to connect.

Minimal information should be collected to improve user trust and sign-in flows. Captive portals in our study that collected optional personal information for marketing purposes were met with abandonment, low trust, or user annoyance. Care should be taken to address why the information is collected and what will be done with it. Personally-identifying information could be stored with trusted entities in order to maximize user trust in safeguarding the information [15].

Female participants in our study expressed higher comfort levels with seeking help to learn about the networks, but some expressed reservations with male members. Initiatives that have strong female representation in providing access, such as Internet Saathi's agents [29], could provide a welcoming experience for women.

As a cautionary note on ubiquitous public Wi-Fi access, some of the underlying fears discussed here could be actualized or exacerbated, such as women's safety online; cybercrime; or fraud. Policy makers and regulators would have to pro-actively consider the effects of unregulated and accelerated expansion of access in an effort to digitize the nation.

Public Wi-Fi as reliable experiences

High-latency and unreliable performances and unintuitive login processes characterized the practical experience of public Wi-Fi access in our study. Captive portals offer the most inclusive legal solution to public access since they work with any browser-capable devices and place no burden on users to install special-purpose software. However, captive portals need to be made usable to be accessible to a wider range of new users and meet regulatory requirements. Easy, secure, and rapid connection experiences provide welcoming experiences to those who seek to connect.

Reliable and high-speed networks are at the core of the network experience. As noted in a study of broadband speeds among Indian families [57], speed is experiential and not necessarily an aspiration- or desire-based driver to a network. Those who did experience good quality networks recalled them as delightful episodes in a sea of spotty networks. While bandwidth is particularly expensive in emerging economies, free but poor quality access did not seem adequate to drive adoption to new network infrastructures. As noted above, many people have other options they already understand and rely upon, even if it means using slow, personal 2G data plans.

Public Wi-Fi as "free" infrastructure

As we have seen, participants had clearly been party to the overwhelming discourse of "free" public Wi-Fi. In the Global North, institutions have a modest obligation to provide amenity service, at a reasonable level of quality and security, to the extent that even normatively illegitimate users routinely take advantage of free Wi-Fi service if they can. In India, we were surprised by the degree to which making service free-of-charge was not enough to convince participants that it was worth taking up.

Public Wi-Fi came with affective costs. There is pleasure in receiving something for free [63], but the frustrations of lack of relevancy, lack of ubiquity, unpredictable performance, and complex user experience relative to the familiar use of purchased mobile data more than balanced it. Public Wi-Fi came with perceived risks—security threats, privacy threats, reputation threats, and health threats. Saving money was not always enough to justify use.

Today's networks are heterogeneous, and the assemblages we rely upon to deliver ubiquitous services now span many technologies and operating entities. As designers we often find we must accept physical 'seams' in infrastructure [21], but the idea that networks themselves might be associated with wildly differing levels of trust and selectively avoided is seen as an idea accepted by only a few studies [13]. This was not the case in our data. While multiple networks now exist in India of today, it still remains a messy, resistant counter to the 'anytime, anywhere' vision [21].

From a socio-economic development point of view, it is unusual to find that 2G mobile data might be seen as preferable to "free, fast" Wi-Fi in developing regions. In some cases, this could be attributed to participants seeing public Wi-Fi as "not free" or "not fast"; but in any case, we can see this as another example of users constructing a "digital repertoire" [18] of usage patterns, suited to their particular circumstances.

CONCLUSION

Indian Internet users are largely familiar with the idea of Wi-Fi, but public Wi-Fi infrastructure is certainly not pervasive and efforts to make it more widely available are significant. We wanted to study users' and non-users' conceptions so that we could understand how likely it was that urban middle-class Indians would instantly take advantage of new Wi-Fi opportunities. What we found is that despite the recent introduction, people came to public Wi-Fi with conceptions shaped by media, popular culture, prior technology cultures and personal or second-hand experiences. As such, these received notions led to vague interest but also reluctance due to specific threats around personal safety, credit balance, health, and device security. Poor experiences further deterred interest. Even prior users of public Wi-Fi expressed concern with connecting to these networks.

While one might assert that the conceptions described here will prove to be ephemeral, it is through action—public awareness, better user experiences, public education, service demonstrations, business model innovation—that they will be changed.

ACKNOWLEDGEMENTS

Our sincere thanks to Vaishali Jain for research support. We thank our participants, the Google Station team, Jose Faleiro, Asif Baki, and our ACs and reviewers.

REFERENCES

1. 2016. IAMAI report. https://goo.gl/Ku53n4. (Feb 2016).
2. 2016. Mexico Connectado website. http://mexicoconectado.gob.mx/. (Sep 2016).
3. Mikhail Afanasyev, Tsuwei Chen, Geoffrey M Voelker, and Alex C Snoeren. 2010. Usage patterns in an urban WiFi network. *ACM Trans. Netw.* 18, 5 (2010), 1359–1372.
4. Syed Ishtiaque Ahmed, Steven J Jackson, Nova Ahmed, and others. 2014. Protibadi: A platform for fighting sexual harassment in urban Bangladesh. In *CHI*. ACM, 2695–2704.
5. Benedict Anderson. 2006. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. Verso.
6. Arjun Appadurai. 1996. *Modernity at Large*. Univ. Minnesota Press.
7. Arjun Appadurai. 2000. Spectral housing and urban cleansing: Notes on millennial Mumbai. *Public Culture* 12, 3 (2000), 627–651.
8. Roger Baig, Ramon Roca, Leandro Navarro, and Felix Freitag. 2015. guifi.net: A network infrastructure commons. In *ICTD*. 27.
9. BBC. 2010. Ghana text hoax predicting earthquake prompts panic. https://goo.gl/kFb6uk. (Jan 2010).
10. Adam Burgess. 2004. *Cellular Phones, Public Fears, and a Culture of Precaution*. Cambridge Univ. Press.
11. Jenna Burrell. 2013. The materiality of rumor. In *Materiality and Organizing: Social Interaction in a Technological World*, Paul M. Leonardi, Bonnie A. Nardi, and Jannis Kallinikos (Eds.). Oxford Univ. Press, 315–332.
12. Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet security perceptions and practices in urban Ghana. In *SOUPS*. 129–142.
13. Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring user confidence in smartphone security and privacy. In *SOUPS*. 1.
14. Elisabetta Costa. 2016. *Social Media in Southeast Turkey*. UCL Press.
15. Rachna Dhamija and Lisa Dusseault. 2008. The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy* 6, 2 (2008), 24–29.
16. Sara Dickey. 1993. The politics of adulation: Cinema and the production of politicians in South India. *J. Asian Stud.* 52, 02 (1993), 340–372.
17. Jill P Dimond, Michaelanne Dye, Daphne LaRose, and Amy S Bruckman. 2013. Hollaback!: The role of storytelling online in a social movement organization. In *CSCW*. 477–490.
18. Jonathan Donner. 2015. *After Access: Inclusion, Development, and a More Mobile Internet*. MIT Press.
19. DoST. 2016. DoST Wi-Fi. https://goo.gl/bNwGVD. (July 2016).
20. Paul Dourish. 2015. Not the Internet, but this Internet: How othernets illuminate our feudal Internet. In *Aarhus Conf.* Aarhus Univ., 157–168.
21. Paul Dourish and Genevieve Bell. 2007. The infrastructure of experience and the experience of infrastructure. *Environ. Plan. B* 34, 3 (2007), 414–430.
22. Michaelanne Dye, David Nemer, Laura Pina, Nithya Sambasivan, Amy Bruckman, and Neha Kumar. 2017. Locating the Internet in the parks of Havana. In *CHI*. ACM.
23. Ericson. 2015a. The Changing Mobile Broadband Landscape. http://goo.gl/Lwgpwk. (Mar 2015).
24. Ericson. 2015b. Girl commits suicide after morphed pics appear on Facebook. http://goo.gl/UGZyfi. (Jun 2015).
25. Firstpost. 2016a. It's business, not personal. http://goo.gl/HbnG10. (Mar 2016).
26. Firstpost. 2016b. Will make Delhi a WiFi city in a year. http://goo.gl/fPd0cK. (Mar 2016).
27. Rob Flickenger. 2003. *Building Wireless Community Networks*. O'Reilly.
28. Laura Forlano. 2009. WiFi geographies: When code meets place. *The Info. Soc.* 25, 5 (2009), 344–352.
29. Google. 2016. Internet Saathi. http://goo.gl/7SDwk2. (Jun 2016).
30. GSMA. 2016. Bridging the Gender Gap. http://goo.gl/517XPf. (Mar 2016).
31. Keith N Hampton and Neeti Gupta. 2008. Community and social interaction in the wireless city: Wi-Fi use in public and semi-public spaces. *New Media & Society* 10, 6 (2008), 831–850.
32. Andrew B Hargadon and Yellowlees Douglas. 2001. When innovations meet institutions: Edison and the design of the electric light. *Adm. Sci. Q.* 46, 3 (2001), 476–501.
33. Lefebvre Henri. 1991. *The Production of Space*. Oxford Univ. Press.
34. HT. 2016. Microsoft CEO in India, to focus on cloud, net connectivity. https://goo.gl/OdR3o5. (2016).
35. IE. 2015. Measuring the Information Society Report. https://goo.gl/efTaaV. (Mar 2015).
36. IE. 2016. Facebook may soon launch cheap WiFi in India. http://goo.gl/poUhL3. (Mar 2016).
37. DNA India. 2015. Digital India: CEOs commit to invest Rs 4.5 trillion. https://goo.gl/xM7smT. (Jul 2015).
38. IT. 2008. IT amendment act. . (July 2008).

39. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. 'My data just goes everywhere': User mental models of the Internet and implications for privacy and security. In *SOUPS*. 39–52.
40. Anandam Kavoori and Kalyani Chadha. 2006. The cell phone as a cultural technology: Lessons from the Indian case. In *The Cell Phone Reader*, Anandam Kavoori and Noah Arceneaux (Eds.). Peter Lang, 227–239.
41. Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, and others. 2009. 'When I am on Wi-Fi, I am fearless': Privacy concerns and practices in everyday Wi-Fi use. In *SOUPS*. 1993–2002.
42. Sri Kurniawan. 2006. An exploratory study of how older women use mobile phones. In *UbiComp*. Springer, 105–122.
43. Brian Larkin. 2013. The politics and poetics of infrastructure. *Annu. Rev. Anthropol.* 42 (2013), 327–343.
44. LiveMint. 2015. Future of public Wi-Fi hot spots in India. https://goo.gl/efTaaV. (Aug 2015).
45. Adrian Mackenzie. 2005. Untangling the unwired: Wi-Fi and the cultural inversion of infrastructure. *Space and Culture* 8, 3 (2005), 269–285.
46. Scott D Mainwaring, Michele F Chang, and Ken Anderson. 2004. Infrastructures and their discontents. In *UbiComp*. Springer, 418–432.
47. Bronislaw Malinowski. 1926. *Myth in primitive psychology*. Norton.
48. Mashable. 2016. Google's free Wi-Fi is now available at 100 railway stations in India. https://goo.gl/epHBKr. (Dec 2016).
49. Arunesh Mathur, Brent Schlotfeldt, and Marshini Chetty. 2015. A mixed-methods study of mobile users' data usage practices in South Africa. In *UbiComp*. ACM, 1209–1220.
50. Joyojeet Pal. 2015. Banalities turned viral: Narendra Modi and the political tweet. *Television & New Media* 16, 4 (2015), 378–387.
51. Alex Pentland, Richard Fletcher, and Amir Hasson. 2004. Daknet: Rethinking connectivity in developing nations. *IEEE Computer* 37, 1 (2004), 78–83.
52. Sundar Pichai. 2016. Bringing the Internet to more Indians. http://goo.gl/P9E9Z3. (Mar 2016).
53. Nandagopal Rajan. 2016. Internet Trends 2016. http://goo.gl/ByYKF2. (Mar 2016).
54. Nimmi Rangaswamy and Nithya Sambasivan. 2011. Cutting Chai, Jugaad, and Here Pheri: Towards UbiComp for a global community. *PUC* 15, 6 (2011), 553–564.
55. Reuters. 2015. Modi revives campaign for digital India. http://goo.gl/7HvbQ5. (2015).
56. Tony Salvador, Genevieve Bell, and Ken Anderson. 1999. Design ethnography. *Des. Manage. Rev.* 10, 4 (1999), 35–41.
57. Nithya Sambasivan, Gulzar Azad, Paul M Aoki, and Saswati Saha Mitra. 2016. We call it Hi-Fi: Exposing Indian households to high speed broadband wireless Internet. In *ICTD*. ACM, 3.
58. Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated technology use in developing communities. In *CHI*. ACM, 2583–2592.
59. Nithya Sambasivan, Paul Lee, Greg Hecht, and others. 2013. Chale, how much it cost to browse?: Results from a mobile data price transparency trial in Ghana. In *ICTD*. ACM, 13–23.
60. Alena Sanusi and Leysia Palen. 2008. Of coffee shops and parking lots: Considering matters of space and place in the use of public Wi-Fi. *CSCW* 17, 2-3 (2008), 257–273.
61. Debhasis Sarkar. 2016. 5 reasons why 4G is not able to excite India. http://goo.gl/fvtWC. (Feb 2016).
62. Ajay Shah. 2012. What security? Costs of KYC outweigh the benefits. https://goo.gl/SQaGSi. (May 2012).
63. Kristina Shampanier, Nina Mazar, and Dan Ariely. 2007. Zero as a special price: The true value of free products. *Mark. Sci.* 26, 6 (2007), 742–757.
64. Vijay Sharma. 2013. Phone Numbers in DND directory. http://goo.gl/usZ75l. (Mar 2013).
65. Smriti Singh. 2016. Delhi gang rape. http://goo.gl/CCrDbZ. (Mar 2016).
66. Thomas N Smyth, Satish Kumar, Indrani Medhi, and Kentaro Toyama. 2010. Where there's a will there's a way: Mobile media sharing in urban india. In *CHI*. ACM, 753–762.
67. Debra Spitulnik. 2002. Rethinking reception through Zambian radio culture. In *Media worlds*, Faye D. Ginsburg, Lila Abu-Lughod, and Brian Larkin (Eds.). Univ. Calif. Press, 337–354.
68. David R Thomas. 2006. A general inductive approach for analyzing qualitative evaluation data. *Amer. J. Eval.* 27, 2 (2006), 237–246.
69. TOI. 2015. A digital dream to put India on information superhighway. https://goo.gl/CxYC2u. (May 2015).
70. TRAI. 2016. The Indian Telecom Services Performance Indicators: January - March 2016. https://goo.gl/vmP1ZX. (Mar 2016).
71. Peter A Valberg, T Emilie van Deventer, and Michael H Repacholi. 2007. Base stations and wireless networks. *Environ. Health Pers.* (2007), 416–424.
72. Rick Wash. 2010. Folk models of home computer security. In *SOUPS*. ACM, 11.
73. Susan P Wyche, Melissa Densmore, and Brian Samuel Geyer. 2015. Real mobiles: Kenyan and Zambian smallholder farmers' current attitudes towards mobile phones. In *ICTD*. ACM, 9.
74. Susan P Wyche, Thomas N Smyth, Marshini Chetty, Paul M Aoki, and Rebecca E Grinter. 2010. Deliberate interactions: Characterizing technology use in Nairobi, Kenya. In *CHI*. ACM, 2593–2602.