New America Foundation

Dialing Down Risks

Mobile Privacy and Information Security in Global Development Projects

By Hibah Hussain*, Open Technology Institute
August 2013

Summary

Over the past decade, mobile phones have become increasingly prominent features of global development projects.[1] Aiming to spur social and economic development in the Global South, a variety of international organizations and nonprofits have invested heavily in mobile-centric projects to address challenges in public health, financial inclusion, transparent governance, and more. Given the high rates of cell phone penetration in the developing world, this trend in information and communication technologies for development (ICT4D) is hardly a surprise.[2]

Many of these mobile-oriented development projects are promising: a recent World Bank report, for example, describes how cell phones are allowing African farmers to access price information via text messages, connecting new mothers to maternal health information, and facilitating interaction between citizens and local governments.[3] However, new technologies bring significant challenges along with benefits. Mobile phones raise pressing privacy and security issues that must be addressed by development practitioners and funders.[4]

Presently, ICT4D practitioners and funders lack any sort of model for best practices, guidelines, frameworks, or discussions about the privacy and security risks raised by mobile development projects. This paper seeks to establish guiding privacy and security principles for mobile ICT4D projects, to provide a framework for project planning and evaluation, and to facilitate productive dialogue and action in the intersection of technology, privacy, and development.

* Hibah Hussain is a Policy Program Associate at the Open Technology Institute. The author thanks researchers at Privacy International and technologists at the Open Technology Institute for their feedback and expertise.

Introduction

From large-scale United Nations initiatives to small, locally-oriented platforms, mobile phones have become increasingly prominent features of global development projects.[1] Aiming to leverage high mobile penetration rates in the Global South for social and economic development, international organizations and nonprofits are launching mobile-centric projects to address challenges in public health, financial inclusion, transparent governance, and more. Although these projects are growing in popularity and scope, key mobile privacy and security risks are rarely addressed by development funders and practitioners.

Mobile information and communication technologies for development (ICT4D) projects generally focus on marginalized and vulnerable communities, meaning that privacy and security gaps can be especially perilous. Most mobile ICT4D users are among the poorest in developing countries: in addition to lacking the means required to make important decisions about the technology they use, they are denied avenues to recourse in cases of privacy harm and breaches of personal data. Additionally, standard privacy and security challenges are exacerbated by issues prominent in much of the developing world, such as high levels of political instability, government corruption, political turnover, unreliable legal systems, and social unrest. All of these factors make it even more difficult to control the effects of data collection, especially when combined with issues like low literacy rates, phone sharing, and other aspects of the status quo in many target communities.

This paper defines personal data as information created by and about users via their use of mobile devices. In addition to encompassing data that is explicitly volunteered by users, personal data includes data that is inadvertently generated by device use (location information, etc.) as well as data that is used to predict future user behavior (financial transactions and credit scoring, for example).[5]

As described later in this paper, political, social, and economic instability in the developing world heightens the impact of privacy breaches and personal data leaks. Even the most optimistic proponents of mobile development projects recognize the risks the projects. pose After extolling mobile data's ability "to

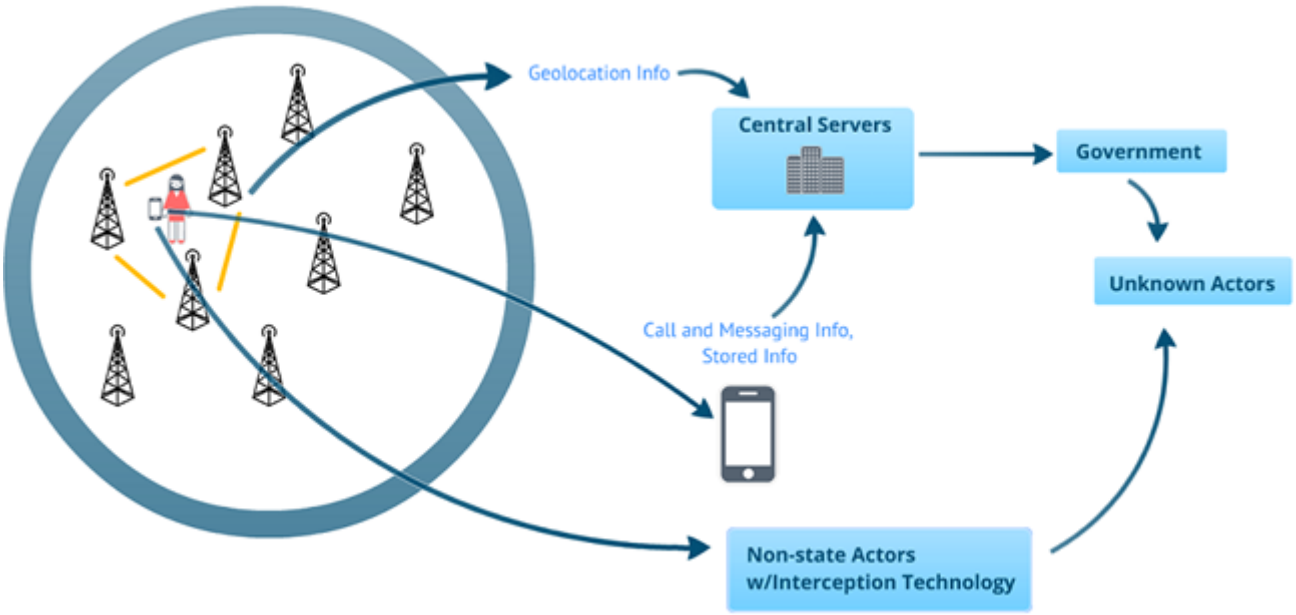

Diagram A: Information Flows in Mobile Networks

detect and monitor epidemics, manage disasters, and optimize transportation systems" in the Global South, an MIT Technology Review article acknowledges that it "will take some careful work to protect privacy and prevent the data from being used in the service of oppression," adding that "you can imagine what Muammar Qaddafi would have done with this sort of data." [6]

Given the sensitive nature of the information being transmitted and the vulnerability of target user communities, it is critical that mobile ICT4D projects take steps to minimize security and privacy risks.

As technologists and mobile security researchers are keenly aware, mobile phones are highly insecure: in order to function, all mobile devices must constantly communicate with cell sites such as towers or mounted base stations, making it impossible to obscure the location of the user. When a phone is used, the nearest cell site logs the phone's ID number along with communications details (call length, etc.) Regardless of whether or not mobile network operators are under government control (as many are) or independent commercial entities, the service providers that run these networks have full access to user information, including location, communications logs, and some stored information. Many of these networks are legally obligated to retain this information for extended periods of time, and it is increasingly easy for third parties to use inexpensive equipment to intercept information transmitted over mobile networks.[7]

Diagram A illustrates the ways in which information flows over mobile networks and how this information can be leaked or intercepted.[8]

Although several technology policy and human rights groups are actively researching and advocating for private and secure communications, most ICT4D projects have yet to meaningfully address these issues. Given the sensitive nature of the information being transmitted by mobile ICT4D initiatives (everything from a user's HIV status to her financial transactions) and the vulnerability of target user communities, it is critical that mobile ICT4D projects take steps to minimize security and privacy risks.

At the moment, ICT4D practitioners and funders appear to lack best practices or guidelines on managing the privacy and security risks raised by mobile development projects. A recent report by the UN Office for the Coordination of Humanitarian Affairs notes that "while private-sector organizations and Government regulators have been grappling with this issue for almost a decade, humanitarian organizations appear further behind."[9] Geared towards ICT4D practitioners and funders, this paper situates the right to secure and private communications within the ICT4D ethos and argues that privacy is a prerequisite for self-determination and socioeconomic empowerment. It then highlights privacy issues that are raised by popular ICT4D initiatives and investigates tangible short-term privacy harms as well as long term privacy concerns in the developing world. Finally, it puts forth recommendations and best practices to facilitate the integration of privacy safeguards into the ICT4D project planning and implementation process.

The concerns and recommendations in this paper span smartphone and basic mobile projects, but it is not this paper's goal to provide granular privacy audits of every genre of ICT4D project. Rather, this paper seeks to:

- Establish guiding privacy and security principles for mobile ICT4D projects,
- Provide a framework for project planning and evaluation, and
- Facilitate productive dialogue and action in

the intersection of technology, privacy, and development.

While this paper's principles and recommendations apply broadly to mobile ICT4D projects, it draws specific examples and lessons from the three most popular mobile ICT4D categories: health, financial inclusion, and governance.

Privacy: A Core Component of ICT4D Goals and Values

Focusing on the values and goals articulated by key ICT4D thinkers and practitioners, this section situates privacy within the ICT4D value system and argues that privacy is a core component of these goals.

The international development sector has evolved tremendously over the past few decades. Unlike the modernist development approaches of the 1950s and 1960s, which focused on top-down aid and centralized decision making, the majority of today's development professionals recognize the importance of supporting self-determination and participation amongst their target communities.[10] Amartya Sen and other key development figures have insisted that development encompasses much more than simple financial or technological aid.[11] Focusing on lasting empowerment, modern development projects aim to build capabilities among underserved communities, ensuring that people have the ability to make meaningful choices and have agency over their lives. Across various sectors, development projects are moving towards more participatory, grassroots models that encourage horizontal information exchange and dialogue between development practitioners and stakeholder communities. Instead of making decisions on the behalf of people, participatory projects emphasize meaningful engagement as a catalyst for individual and community empowerment. [12]

During a recent presentation at Harvard's Berkman Center for Internet and Society, ICT4D researcher and practitioner Dr. Dorothea Kleine operationalized Sen's capabilities approach, highlighting ways to build choice into ICT4D projects. Kleine, who leads the ICT4D Centre at Royal Holloway University of London, noted that development projects should "expand the freedom that people have to live the lives that they themselves value."[13] Technology-oriented development projects can work towards this goal via transparent technology and participatory design and implementation.

In an increasingly digital world, the ability to know and control how information about oneself is collected, used, and shared with the world is a crucial component of self-determination. Noting that governments are increasingly relying on digital data from private corporations to categorize citizens based on their political leanings, minority status, economic backgrounds, health information, and more, privacy-oriented advocacy groups have linked concerns about privacy to fundamental development and human rights issues.[14] For example, privacy breaches and surveillance have been linked to social and economic discrimination. Privacy International's recent paper on surveillance in the Global South describes the ways in which digital surveillance "often amounts to a form of social sorting, whereby governments use controls to create and reinforce social differences and other forms of discrimination, or undermine the enjoyment of other human rights."[15] This sorting could easily be enhanced by health information collected by well-meaning development agencies, which could be leaked or intercepted and be used to illicitly monitor abortions, pregnancies, HIV statuses, and more. This information can then have a wide range of social, economic, and political effects, impacting an individual's ability to get a job, vote, get a loan, or even continue living in her community.

Given these links between data collection, personal safety, and sociopolitical power and agency, it is

critical for users in the developing world to be able to control the data that mobile phones collect about them. In the modern global economy, the ability to control and understand data is directly connected to social, political, and economic control. "Personal data is the new oil of the Internet and the new currency of the digital world," notes European Consumer Commissioner Meglena Kuneva, pointing to the links between digital data and socioeconomic agency.

Some global governance groups are beginning to recognize these links between development, democracy, and digital privacy. In a recent publication, the OECD argues that "efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy."[16] Noting that democracy and openness hinge on the ability to speak freely without fear of surveillance, retribution, or future harm, researchers assert that "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship." Unfortunately, as the Electronic Frontier Foundation (EFF) notes, some states have made surveillance and data interception easier than ever: India, for example, has limited users' abilities to encrypt data, and the Colombian government requires telecommunications networks and providers to ensure that state interception is possible at all times. Furthermore, these providers must retain user data for five years, including identity, address, geographic location, and more.[17]

Even in states without such streamlined interception and surveillance mechanisms, mobile networks are vulnerable to surveillance via cheap equipment.[72] Given the high level of vulnerability inherent to mobile networks, mobile ICT4D projects can never take user privacy for granted and must take steps to minimize risks that might result from breaches or leaks of sensitive data. Ultimately, ICT4D projects aim to level the playing field: they are rooted in the belief that human beings have equal rights regardless of location and assets. Although privacy protections are far from perfect in the developed world, there is recognition that sensitive data and information ought to be protected.[18] Given the assertion that "future goals must reach beyond traditional development thinking to...apply to poor and rich countries alike," communities in the developing world should be afforded the same attention to privacy and security protections.[19]

Assessing The Risks

This section summarizes risks associated with mobile communication, including but not limited to smartphone apps/projects. It drills into specific genres of mobile ICT4D projects, outlining the particular risks posed by mobile health, finance, and governance ICT4D initiatives. In addition to summarizing popular ICT4D projects in these sectors, this section highlights harms that have resulted from inadequate privacy protections.

Popular mobile ICT4D projects span a range of sectors, but mobile health, finance, and governance projects are especially prominent.[20] All of these varied projects and applications are susceptible to the general risks for mobile outlined above, but each category of mobile projects is accompanied by unique privacy and security risks.

Mobile Health

Lauded for their ability to provide medical care to remote and poor users, track epidemics, and monitor long-term diseases, these projects are being deployed throughout the Global South. These projects include epidemic tracking, medical appointment reminders, and telemedicine platforms. In addition to sending voice or text messages describing a user's health, many mHealth applications use low-cost medical imaging systems to send their data and images to a central processor, where they can be combined and analyzed

to provide a full picture of the patient's health.[21] In addition to promoting general best practices for a healthy lifestyle, the majority of mHealth applications have a specific area of focus, such as maternal health or specific infectious diseases.

The data being transmitted through these applications is extremely sensitive; for example, mobile HIV monitoring and medication reminders are being used in communities throughout Kenya, Malawi, South Africa, Mexico, and other countries.[22] These applications, which are being deployed by international development agencies and nonprofits, send daily reminders to HIV-positive patients detailing their anti-retroviral therapy schedule. They also allow community health workers to send information about a patient's HIV status directly to project managers.[23] This ability to provide medical care to vulnerable populations is promising, but it is accompanied by incredible risks. There have been documented cases of governments requesting this information: recently, the Haitian government demanded that the public health organizations working in the country hand over the medical records of all patients infected with HIV. This information was to be used to create a national database that would track the prevalence of HIV among Haitian citizens.[24] In addition to the discrimination and violence that might result from such a database, this example is especially disconcerting because there are no guidelines on how the database might be used. It is also worth noting that for every similar reported incident, there are numerous government requests that are never made public.

In addition to government requests and data leaks or breaches, mHealth projects must also contend with national policy landscapes that make it impossible to provide discreet, safe care to patients. VidaNet, an HIV patient reminder system that was being deployed in Mexico City, illustrates this point. Despite the project's dedication to patient privacy, Mexico's ongoing focus on SIM card registration is making it virtually impossible to transmit sensitive information over mobile devices anonymously.[25] Since SIM card registration links every mobile device to a specific citizen, sensitive user health data can easily be linked to a user's identity, address, and other information that the government possesses. Finally, mHealth projects must deal with the reality of human error and leaks. The more people (community health workers, doctors aides, etc.) who have access to mobile data, the more likely it is that sensitive data will be misused or leaked. Furthermore, human and mechanical errors present formidable problems: a recent research survey on mobile AIDS platform users reports that "a fifth (18%) of participants reported that someone else had inadvertently received their IVR or SMS" containing AIDS and HIV information.[26]

Since SIM card registration links every mobile device to a specific citizen, sensitive user health data can easily be linked to a user's identity, address, and other information that the government possesses.

Mobile Finance

Mobile money and financial inclusion projects comprise another category of promising yet problematic ICT4D endeavors. Mobile payment platforms can facilitate person-to-person, government-to-person, person-to-business, and business-to-business payments, while mobile banking platforms allow users to participate in a range of innovative savings and credit programs. Furthermore, researchers have described how mobile payment platforms can be used to build credit profiles and give users access to loans.[27] This can certainly be valuable, but if mobile payment data is used to classify users' creditworthiness, users should be fully aware of how their mobile payment transactions are tracked, and how this data affects their credit profiles.

Many mobile finance projects, if not most of them, are structured as public-private partnerships, wherein governments and nonprofits partner with commercial groups to provide services.[28] Such partnerships can be efficient in the short term, but they necessitate more data sharing between a larger number parties, thereby increasing the potential for long term data leakage and unauthorized sharing as data travels across and within disparate internal databases. This increased information sharing between public and private entities is further complicated by government biometrics initiatives, many of which are explicitly linked to financial inclusion projects, including mobile money projects. Many projects, such as India's Project Aadhaar, link this biometric data to mobile banking for the underserved.[29] Project Aadhaar, which is building "a universal ID system for all citizens, including iris scans, ten fingerprints, and a picture of each face"[30], features a strong mobile component: the Unique Identification Authority of India (UIDAI) is partnering with several banks and Visa to launch the Saral Money bank account service. This service uses Aadhaar's biometric authentication to allow citizens without access to formal banking structures to use debit cards or mobile phones to access banking services.[31] The project's emphasis on mobile is clear: it plans to spend nearly $1.2 billion dollars (Rs 7,000 cr) to distribute free smartphones to the poor and to "move most of its service delivery to the mobile platform starting next year."[32] This trend is not limited to India: the Center for Global Development estimates that over 450 million citizens of developing countries have had their biometric data recorded, and projects that this number will triple in the next five years.[33]

This combination of personally identifiable information and the tracking of all financial transactions is incredibly potent, especially if the data collectors can combine it with other information collected by mobile phones (health, location, communications, etc.). Another enormous problem with this sort of identifiable, centralized data is that breaches/leaks cannot be contained: with every piece of data tied together and to a specific identity, it is nearly impossible for sensitive information to be isolated and de-identified. These risks are heightened by outdated infrastructure and organizational challenges.[34] As researchers and technologists Nathan Eagle and Joshua Blumenstock have noted, "having a detailed repository of information on an individual...is a delicate matter in any context. However, in developing countries, where many individuals are economically vulnerable, legal institutions are often fragile, and certain political freedoms cannot be taken for granted, these concerns are particularly important."[35] A recent description of the Aadhaar project attests to this point, describing the organizational challenges faced by the program. "Hundreds of new Aadhaar ID cards are strewn in messy piles on the counter of a small tea-shop on the edge of the village," describes an article on how the program is being implemented, "locals drift in and rifle through the cards, looking for their own."[36] This sort of disorganization and lack of security is incredibly problematic, especially given the sensitive nature of the information tracked by the project. Aadhaar focuses primarily on finance, but the project also has strong governance goals: part of its objective is to bridge the distance between governments and underserved citizens.

Mobile Governance

Aiming to make government more accessible and participatory, mobile governance projects allow citizens to contact law enforcement, participate in political debates, report community needs, and much more. Serving as platforms for whistleblowing, voter registration, and government information sharing, these applications aim to facilitate citizen engagement and government accountability. However, these applications will not be successful on a large scale unless ICT4D practitioners are able to assure users that their data is securely transmitted and scrubbed of all personally identifying

information before storage. This is a monumental task given mandatory SIM card registration and information sharing between mobile operators and government agencies. However, without a guarantee of privacy, these mobile governance platforms could be counterproductive and even dangerous. The World Bank notes that "citizens might seek anonymity (or pseudonymity) as they become more vocal to avoid the risk of reprisals due to their views" and that "governments may need to consider which services require identification and which services (anticorruption hotlines, for example) might be more popular if citizens can remain anonymous when they make a report."[37] Unfortunately, this recommended anonymity is in tension with the policies and technical issues discussed above.

In many communities, today's corrupt officials can easily become tomorrow's government leaders. In order to secure his hold on power, a savvy politician's first order of business after assuming office might be to come after the citizen whistleblowers who reported him via a mobile governance platform. "Information that identifies people who report on acts of violence can be used by governments or armed groups for retribution," notes a recent UN report on humanitarianism in the networked age. Describing threats to aid workers responding to floods in Pakistan, the report notes that "even seemingly innocent information, such as the location of food distribution points and clinics, can attract violence."[38] Such scenarios may seem extreme, but there are an unfortunate number of examples of mobile data leading to politically-motivated violence and incarceration. Take, for example, the anti-government food protests in the Egyptian town of Mahalla el-Kubra in 2008, during which many protesters used their mobile phones to make calls and send messages. After the protests, which were a response to government policies associated with rising food prices, the Egyptian authorities compelled Vodafone to hand over customer communications data, leading to the conviction of twenty-two protesters.[39] Although these protests were not a direct result of an ICT4D project, they illustrate the ease with which mobile data can be intercepted and used to punish civil disobedience.

These risks are heightened by emerging systems that facilitate widespread government surveillance of mobile networks. India's Central Monitoring System (CMS), which the government began rolling out in April 2013, provides a prime example of how governments are expanding the breadth and depth of their surveillance capacities. The system is in its early stages, but it aims to provide the Indian government with "centralized access to the country's telecommunications network," facilitating the "direct monitoring of phone calls, text messages, and Internet use by government agencies."[40] Allowing agencies to bypass service providers, the CMS will be able to access each of India's 900 million landline and mobile phone users and 120 million Internet users.[41] Despite the system's broad scope, there are few regulations or processes in place to prevent government misuse and protect user rights. Human rights advocates are especially concerned about how the CMS might be used to target journalists, activists, and citizens of opposing political parties. "The Indian government's centralized monitoring is chilling, given its reckless and irresponsible use of the sedition and Internet laws," notes Cynthia Wong, Senior Internet Researcher at Human Rights Watch.[42]

"Information that identifies people who report on acts of violence can be used by governments or armed groups for retribution," notes a recent UN report on humanitarianism in the networked age.

Thus far, the privacy concerns detailed in this paper have primarily focused on the immediate harms that result from privacy and security oversights. However, these immediate harms are just the tip of the iceberg: numerous researchers have demonstrated the impact

of aggregating mobile data over time. Take, for example, a recent study on human migration patterns within Rwanda. The researchers obtained a log of all phone activity over three years in Rwanda from the country's primary telecommunications operator. They then examined the number of cell towers used by each phone owner over a specific period of time and combined this data with the maximum distance traveled between towers. As mentioned, mobile phones must communicate with cell towers at all times in order to function. Their study yielded detailed, accurate migration predictions and reinforced other researchers' findings that given partial information about a user's location and movement patterns, it is very easy to reconstruct movement patterns and predict future movement.[43] Leveraging this information, they were able to infer patterns of internal migration that had eluded even the Rwandan government.[44] This sort of data aggregation and analysis can be incredibly useful when it is being executed by ethical researchers working under stringent Institutional Review Board (IRB) guidelines, but it is problematic when such large-scale data is collected and analyzed by groups that are under no obligation to use it transparently and ethically. Even as they describe the potential benefits of mobile data collection, Eagle and Blumenstock argue that privacy concerns are pressing, especially with regards to "data that is unobtrusively collected, and for which it is often impractical to obtain the informed consent of the subjects under study." [45]

Of course, even when user consent is obtained, the cumulative and unpredictable nature of long-term privacy harms makes it difficult to control damage. As law professor and digital privacy expert Daniel Solove points out, "people may agree to many forms of data collection, use, or disclosure over a long period of time, and the harmful effects may emerge from the downstream uses of the combination of the data." [46] Additionally, notice and consent is especially difficult in developing communities. Recently, the London School of Economics published what continues to be one of the only papers focusing on the privacy concerns raised by mobile health projects. Highlighting the limits of notice and consent in ICT4D projects, the paper notes that in most target communities, "neither the patients nor the practitioners are particularly aware of rights and responsibilities," and that "literacy may be minimal, so notices are insufficient."[47]

All of these concerns and risks are magnified by the ubiquity of phone sharing in the Global South. Unlike much of North America and Europe, where phones are viewed as private to their owners, dynamics are far more complex in many developing communities. In a first-of-its-kind study on phone sharing in the Global South, Dr. Jenna Burrell of UC Berkeley's School of Information maps a variety of sharing and usage patterns in Uganda. Highlighting the nuanced differences between how phones are used and shared in communities, Burrell distinguishes between a phone's purchasers, its users, its operators, its possessors, and its owners.[48] Burrell's categories often overlap, but their granular distinctions attest to a complex sharing ecosystem: as phones are passed between people who have varying degrees of access to and control over the information stored on them, traditional notions of digital privacy become increasingly complicated.

As phones are passed between people who have varying degrees of access to and control over the information stored on them, traditional notions of digital privacy become increasingly complicated.

As mobile ICT4D practitioners and funders launch projects, it is important to remember that privacy and security issues are affected by power relationships and the social norms that govern gender roles, marriage, courtship, and sexuality. Even when mobile phones "belong" to/are purchased by women, men often insist on reviewing or controlling phone usage. In rural Uganda, for example, many women "reported

almost complete exclusion from phone operation."[49]. These informal power structures are especially problematic given the proliferation of mobile health applications that focus on reproductive, maternal, and sexual health. These applications collect and transmit a range of information. Some examples of information transmitted by mobile health applications include birth control usage, sexual health and history, and paternity information. This information, which is often transmitted in the form of appointment reminders, medication alerts, or test results, can suggest sexual behavior that a user may not want disclosed, such as extramarital affairs, homosexuality, or sexually transmitted diseases. In addition to fueling discrimination and stigma, this information might also catalyze emotional and physical harm. "Sexuality is a sensitive topic in nearly all cultures," note mobile health researchers from the London School of Economics, "but the ramifications of wrongful disclosure in some contexts may result in severe actions being taken against individuals, sometimes even involving death." [50]

Given that digital risks vary greatly depending on communities and users, it is impractical to create an exhaustive account of all potential risks raised by specific social, political, and economic landscapes and norms. Rather, pre-project research is a more effective method to address these risks. Prior to launching mobile projects, ICT4D practitioners should consult local partners, regional groups, and existing resources in order to gain a fuller understanding of the social and political landscapes that will affect how users interact with mobile projects.

The Gap Between Privacy and ICT4D Worlds

This section is based on a review of the ICT4D field. Focusing on important mobile ICT4D resources, convenings, and dialogues, this section highlights the extent to which privacy is generally left off the ICT4D agenda. It then segues into the risks related to mobile ICT4D projects.

Upon examining leading ICT4D journals, conferences, and resources, a clear trend emerges: even as mobile projects receive an increasing amount of attention, the privacy and security issues that accompany mobile devices are insufficiently addressed. A content analysis of several leading ICT4D journals and conference programs is a helpful way to appraise the extent to which mobile privacy issues are currently being discussed by the ICT4D community. Background research for this paper included reviewing leading ICT4D journals, articles, and conference agendas to for mentions of mobile privacy and security issues.

With the exception of a handful of groups such as Privacy International, Bangalore's Centre for Internet and Society, and Harvard Law School's Berkman Center for Internet and Society, very few groups are actively engaging with the privacy and security aspects of ICT4D projects. As the aforementioned mobile health report from the London School of Economics notes, "where poor privacy practices may make already vulnerable people even more vulnerable, privacy is often perceived as an impediment to their care. Where it matters most is where it is mostly ignored."[51]

Prior to launching mobile projects, ICT4D practitioners should consult local partners, regional groups, and existing resources in order to gain a fuller understanding of the social and political landscapes that will affect how users interact with mobile projects.

Occasionally, individuals and groups outside of the developing world will argue that privacy is less valued by communities in the Global South. In addition to being highly questionable as to its accuracy, this assertion has little bearing on whether or not users should be able to understand and control how their data is shared. Users across the world may differ in

their approaches to privacy issues, but they share the right to affect how their personal information is collected and with whom it's shared. Several empirical studies indicate that when mobile data collection and sharing mechanisms are explained to users in the Global South, they become deeply concerned about privacy issues. "Indians are largely unaware of the extent to which databases of personal information are sold and traded among companies," notes a recent survey-based research study. "When informed of this practice...individuals are often shocked and outraged."[52]

A growing number of technology and media-oriented development groups are beginning to recognize the negative impacts of overlooking privacy in media and technology oriented projects. In February 2013, for example, the Center for International Media Assistance (CIMA) hosted an event to explore the impact of digital security and privacy issues in Latin America. The event explored the findings of a paper by Freedom House and the International Center for Journalists surveying digital and mobile security among Mexican journalists and bloggers. Warning that "corrupt actors are using new technologies to identify and monitor those who may speak out against them," the survey found that as journalists and bloggers "increasingly use online platforms, social networks, and mobile devices to post comments or reports about crime and corruption, they face serious digital risks to their identity and privacy."[53]

"Corrupt actors are using new technologies to identify and monitor those who may speak out against them."

Despite the report's focus on journalists and bloggers, its main points are also relevant to ICT4D practitioners and funders who work outside of governance or journalism-oriented mobile ICT4D projects. First of all, the report highlights the extent of the gap between a user's technological skills and his or her understanding of privacy issues: the fact that journalists, most of whom are far more educated and experienced than the average ICT4D target user, cannot manage digital privacy and security risks is deeply problematic. It highlights why privacy awareness and understanding must be incorporated into mobile ICT4D projects from the very beginning. Secondly, the report and ensuing CIMA event clearly link digital harms to physical violence and other grave "real world" repercussions. After detailing the many ways in which mobile information has been misused by drug cartels, local law enforcement, organized crime groups, and political opponents, the report argues that "mobile insecurity has become a new and uncontrolled source of danger to the physical and psychological safety of independent journalists and bloggers alike." [54]

The survey also highlights why formal legal procedures have been unable to ameliorate these harms. The realities of cartel-police cooperation and corruption within telecommunications operators and government bodies make it impossible to regulate data in any meaningful way. Even in the absence of blatant corruption and organized crime, however, formal legal structures are ill-equipped to handle the complex, ever-changing world of data privacy and security.

Beyond The Law: The Shortcomings of Purely Legal Approaches

This section highlights existing legal protections for mobile data in the developing world, noting that the handful of ICT4D groups thinking about privacy issues are taking a purely legal approach. This section unpacks why a purely legal approach provides insufficient privacy protections to ICT4D stakeholders, and lays the groundwork for the solutions and recommendations in the paper's next section.

Although a handful of mobile ICT4D projects are actively grappling with mobile data privacy and security issues, the majority of these groups are limiting themselves to existing legal frameworks in their target communities. These projects ask: what legal frameworks govern mobile privacy and security issues? How can we ensure that mobile ICT4D projects comply with legal data protection and security issues? Such questions are undoubtedly useful: often, they prompt the examination of national legislation and international standards and agreements. However, focusing exclusively on legal compliance is inadequate, especially given the fact that privacy laws across the world are often minimal, confusing, conflicting, and impossible to enforce.

Privacy issues are directly addressed and protected in human rights law and agreements, but most of these are soft guidelines rather than enforceable laws. Some of the earliest guidelines for data privacy were published by the Organization for Economic Cooperation and Development (OECD) in the late 1980s.[55] These guidelines include recommendations for limiting the collection and use of data, maintaining data quality, specifying the purpose of data collection, implementing effective security safeguards, and facilitating transparency, accountability, and user participation in data governance.

The OECD guidelines inform many existing international privacy recommendations and national policies, and have paved the way for Article 12 of the United Nation's Universal Declaration of Human Rights, which asserts that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence" and that "everyone has the right to the protection of the law against such interference or attacks."[56] Similar language protects privacy in Article 8 of the European Commission on Human Rights.[57] International development projects vary greatly based on goals, funders, and communities, but given the sector's strong commitment to global human rights, these normative privacy principles are of crucial importance.

Unsurprisingly, national privacy laws vary greatly. However, even nations with comparatively robust privacy laws find it incredibly difficult to actually enforce these laws in meaningful, coherent, and effective ways. For example, North American and European nations have articulated privacy protecting principles and have assembled working groups and initiatives to address problems and gaps in privacy law. [58] These frameworks, laws, and reform efforts are far from perfect, but they're more substantial than what exists in developing communities. Despite these efforts, however, privacy protection remains impractical, fragmented, and confusing even in these nations. The United States is no exception. As Solove recently noted, "U.S. privacy law is so muddled that it can't provide clear answers about how most types of data are protected."[59]

In the United States, the Fourth Amendment plays a critical role in determining the scope of government information gathering on citizens. The Fourth Amendment guards against unreasonable search and seizure by government and/or law enforcement. In court, Fourth Amendment decisions hinge on reasonable expectation of privacy tests, which are often problematic in their subjectivity.[60] A key factor in determining whether or not one's expectation of privacy is reasonable and protected by the Fourth Amendment is whether or not information is "knowingly exposed" to a third party or the larger public. However, these principles underpinning the Fourth Amendment are complicated by new systems of data collection and sharing. For example, although users may "knowingly expose" a great deal of information to third parties via social networks, loyalty programs, and mobile apps, they are often unaware of how this information might be combined with other sources of personal information and/or shared with other third parties, including government agencies. "The Framers of the Constitution likely

had no idea the Fourth Amendment would serve as the foundation for regulation our entire system of law enforcement," notes Solove, describing judicial decisions made under the Fourth Amendment as "riddled with inconsistency and incoherence" and "lacking a progressive understanding of privacy in light of modern technology." [61]

As problematic as the Fourth Amendment is, the legal frameworks governing corporate tracking are even less cohesive and coherent. There are no overarching processes or authorities to handle corporate tracking issues. Instead, issues are discussed and addressed as they arise, leading to siloed, fractured, and inconsistent decisions. For example, despite the World Wide Web Consortium (W3C)'s attempts to reach a consensus on web tracking, very basic web tracking issues remain unresolved. How, for example, should Do Not Track mechanisms be implemented? What constitutes invasive tracking? What constitutes meaningful consent?[62] The Consortium's web tracking efforts have been so fruitless that participants are now discussing how to end the efforts as quickly as possible. "I think it's right to think about shutting down the process and saying we just can't agree," notes Jonathan Mayer, a Stanford-based digital privacy researcher and W3C tracking group participant.[63]

Keeping these legal shortcomings in mind, mobile ICT4D funders and practitioners must be proactive rather than reactive with regards to user privacy.

Meanwhile, other digital privacy issues are being handled by disparate groups via completely distinct processes: the National Telecommunications and Information Administration (NTIA) is working on mobile application privacy,[64] the Federal Trade Commission is handling social network privacy breaches,[65] and members of Congress are exploring the privacy implications of emerging technologies like wearable digital devices.[66] Faced with this combination of contradictory legal precedents and ad hoc processes, even nations with dedicated legal structures and statutes cannot rely solely on the law to protect privacy. In developing countries, most of which lack these formal laws, structures, and bodies, legal compliance with privacy laws proves to be utterly insufficient for protecting user privacy. As Carly Nyst, Head of International Advocacy at Privacy International, explains, "in many developing countries [legislative] frameworks are either at a nascent stage, are not implemented or enforced, or simply do not exist at all."[67]

Although several developing nations have signed onto international privacy-protecting treaties and participated in conventions, these principles are not codified in enforceable laws. Furthermore, the existence of laws is rarely sufficient to protect privacy: "laws may exist but the regulations that give life to these legal rights may not have been codified, and the ability to gain access to remedies may be limited," notes a white paper on digital medical privacy in the developing world.[68] What's more, existing regulations may be sidestepped via bribery, or they may be altered in the aftermath of political or social emergencies and changes in political power. Keeping these legal shortcomings in mind, mobile ICT4D funders and practitioners must be proactive rather than reactive with regards to user privacy. From implementing technological safeguards to integrating privacy and security audits into project planning, ICT4D projects need to take concrete steps in order to protect the personal information of their stakeholders. The following section details technical and policy-oriented privacy and security recommendations for mobile ICT4D funders and practitioners.

Safe and Secure ICT4D: Recommendations and Guidelines*

This section highlights core principles that can guide ICT4D funders and practitioners as they

*The author thanks Brian Duggan at the Open Technology Institute for contributing content and feedback to this section.

seek to incorporate privacy protections into their projects. In addition to outlining existing frameworks and best practices, this section proposes standards that can be built into privacy audits and/or peer reviews for mobile ICT4D projects.

When seeking to integrate meaningful privacy and security safeguards into ICT4D projects, the sheer number of stakeholders and actors in the ICT space presents a challenge. This paper acknowledges that governments, telecommunications companies, and digital service providers can and should play key roles in the protection of mobile privacy and security. However, the recommendations below are geared specifically towards ICT4D funders and practitioners working with mobile technology in the developing world. Unlike governments and private companies, who have myriad resources and regulations to address how mobile data can and should be collected, used, and shared, ICT4D funders and practitioners lack a framework with which to audit and promote privacy in ICT4D projects. Drawing from the Fair Information Practice Principles, the OECD Privacy Principles, and privacy criteria implemented by government agencies and the private sector, the following standards and benchmarks provide a normative framework for mobile ICT4D projects.

As mobile technology becomes an increasingly important feature of public and private projects, government and industry groups are actively developing privacy principles to protect user data and engender user trust. These principles include transparency, redress, specification for purpose of data collection, limitations on data retention and use, standards on data quality and integrity, employee trainings, and internal and external accountability and auditing.[69]

The values and user rights listed below are rooted in the core ICT4D principles of self-determination and participation. The first column addresses knowledge and transparency issues: it articulates what mobile ICT4D users need to know in order to make meaningful decisions about their data. Focusing on agency and control, the second column details the actions that users should be able to take in order to have agency over how their data is collected and shared. These values and user rights are followed by a list of responsibilities for ICT4D practitioners and an accompanying criteria checklist for funders.

Values and User Rights	
Knowledge and Transparency	Agency and Control
• Users should know how mobile ICT4D data collection systems operate. • Users should know how and with whom personal information might be shared. • Users should know when new information is collected and/or shared.	• Users should have to consent to data collection and sharing before any information is collected. • Users should have the ability to access, audit, and amend their personal data. • Users should have the ability to hold data collectors responsible for gross negligence, misuse, and/or harm resulting from data collection/sharing outside of the scope of the project.

Guiding Principles for ICT4D Practitioners and Funders

Principle 1: Address Surveillance Risks

Projects should take steps to ensure that user data is secure from third party surveillance.

- What due diligence is exercised in researching and understanding the policy landscape of target communities?
- Does the project examine the relationships between mobile carriers and government surveillance structures prior to launch?
- Does the project have procedures in place to vet local partners for transparency and ethics?
- Does the project allow accounts without real-world identifiers (such as real names, government ID numbers, etc.)?
- Does the project have a data retention plan detailing how long collected data will be retained and how it will be stored?
- Does the project train employees, partners, and contractors to understand best practices regarding privacy and information security?
- Does the project consider particular ethnic, religious, social or cultural contexts and adapt its data collection practices accordingly?

Principle 2: Limit Data Collection and Use

Mobile ICT4D projects should limit data collection to what is absolutely necessary for the project's goals.

- Does the project take steps to ensure that practitioners only have access to the least amount of data necessary to do their jobs?
- Does the project retain only the data that is needed for long term analysis? (For example, projects can aggregate and analyze data as it is received in short intervals and then sanitize this data to securely retain only what is needed for future analysis.)
- Does the project define how collected data may or may not be used in the future?

Principle 3: Promote and Facilitate Transparency

Mobile ICT4D projects should be transparent about what data is collected, how it is shared, and how it might be used in the future.

- Does the project notify users when data is collected? What mechanisms are in place to ensure that these notifications are understandable and thorough?
- Does the project disclose which third parties and partner groups might also have access to collected data?
- Does the project keep audit trails of which employees, volunteers, and partners have access to which data sets?

Principle 4: Incorporate User Feedback

In addition to addressing user questions and concerns, mobile ICT4D projects should give users the ability to access, amend, and/or delete their data.

- What steps does the project take to ensure that individuals understand privacy and security risks prior to becoming mobile ICT4D users?
- What mechanisms exist for integrating user concerns and feedback into the project?
- Does the project allow for granular data deletion and account deletion at any point during or after the project cycle?
- Does the project allow complete data download in portable formats?

Principle 5: Assume Responsibility

Mobile ICT4D projects should assume accountability for potential risks and harms incurred via their projects and platforms.

- Does the project detail procedures for privacy risk assessments and audits?
- Does the project detail methods to address security issues immediately and effectively?
- Does the project identify mechanisms to provide recourse to users in the case of privacy harms?

Concluding Notes and Next Steps

The last few years have witnessed a great deal of excitement regarding the ways in which mobile phones can address development challenges.[70] It is certainly true that mobile phones play critical communications roles in the Global South, connecting users to one another as well as local and global communications networks. Innovative mobile health, finance, and governance projects have the potential to connect some of the world's most vulnerable and underserved communities to critical information and platforms. However, new mobile projects are accompanied by new ethical risks and responsibilities, many of which are amplified in unstable and resource-scarce communities. In addition to serious immediate risks (for example, harmful uses of leaked sensitive personal information), mobile privacy and security oversights raise long term concerns regarding data ownership, sharing, and profiling.

On its own, mobile technology cannot automatically solve development challenges; in fact, as this paper describes, it might actually create new problems. In order to acheive lasting and positive socioeconomic change, the deployment of mobile technology in the developing world must occur in tandem with thoughtful, well-researched policies, informed design, and community engagement. As a recent paper on big data for international development notes, "the exploration of data-based knowledge to improve development is not automatic and requires tailor-made policy choices that help to foster this emerging paradigm."[71] This paper highlights top-level technical and policy best practices, but it acknowledges that there is a lot more work to be done. Promoting mobile privacy and security requires active commitment and cooperation between service providers, governments, nonprofits, foundations, and researchers.

Given this complex ecosystem, it will be a challenge for even the most capable mobile ICT4D practitioners and funders to ensure mobile security and privacy. However, every privacy-protecting step taken by practitioners and funders makes a crucial difference: for example, the decision to store a piece of data without real-world identifiers may end up protecting a user from stigma in the event of a data breach or leak. Following the recommendations outlined above is critical for minimizing risks and harms in target communities, but expanding and updating these recommendations is vital as mobile ICT4D initiatives become even more widespread and powerful. More specifically, the following questions should be addressed at ICT4D and privacy convenings: what additional privacy and security risks are posed by unstable social and political environments, and what are effective ways to approach these risks? What are the most effective ways of holding practitioners accountable for observing best technical and policy practices? What are the best ways to ensure that ICT4D users have meaningful control over the data they generate?

To be sure, no single policy or technical solution can guarantee full privacy and information security. This paper addresses a very specific and narrow set of issues, and recognizes that fully addressing the privacy and security issues raised by mobile phones will require significant action and collaboration between a variety of global actors. Still, the fact remains that even as we better understand the need for information security in the developed world, more and more technology is being deployed in Global South with no mention of privacy or security. Given the risks and challenges highlighted in this paper, we can no longer assume that technology will automatically aid the developing world and start thinking about how we can incorporate privacy and security safeguards into development projects and platforms. Otherwise, privacy and security challenges may overshadow the many benefits that mobile ICT4D initiatives have to offer.

Works Cited

[1] ICTWorks By Inveneo, "ICT4D is Responding to Changing Technology." Accessed Mar. 26, 2013. http://www.ictworks.org/2011/09/23/responding-changing-technology

[2] Fitzpatrick, Alex. "75% of World Has Access to Mobile Phones [STUDY]." Mashable. Last modified Jul.18, 2012. Accessed Feb . 20, 2013. http://mashable.com/2012/07/18/mobile-phones-worldwide

[3] International Bank for Reconstruction and Development / The World Bank, "Information and Communications for Development 2012: Maximizing Mobile." Accessed May 1, 2013. http://go.worldbank.org/0J2CTQTYP0.

[4] *Information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks.* OECD Guidelines for the Security of Information Systems and Networks. Paris, France: OECD Publications, 2002. www.oecd.org/internet/ieconomy/15582260.pdf p.13

[5] *Personal Data: The Emergence of a New Asset Class*. Geneva, Switzerland: World Economic Forum with Bain and Company, 2011. https://www.privacyassociation.org/resource_center/personal_data_the_emergence_of_a_new_asset_class p. 7

[6] Talbot, David. "Big Data from Cheap Phones." *MIT Technology Review*. Apr. 23 2013. http://www.technologyreview.com/featuredstory/513721/big-data-from-cheap-phones

[7] Tactical Technology Collective and Frontline Defenders, "Security in a Box: Mobile devices and security ." Accessed Mar. 2, 2013. https://securityinabox.org/en/chapter_10_1

[8] Electronic Frontier Foundation, "Surveillance Self Defense: Mobile Devices." Accessed Jun. 1, 2013. https://ssd.eff.org/tech/mobile

[9] UN Office for the Coordination of Humanitarian Affairs (OCHA), "Humanitarianism in the Network Age." Accessed Apr. 6, 2013. https://ochanet.unocha.org/p/Documents/WEB Humanitarianism in the Network Age vF single.pdf p. 40

[10] Manyozo, Linje. (2006) "Manifesto for Development Communication: Nora C. Quebral and the Los Baños School of Development Communication". Asian Journal of Communication 16 (1): 79–99.

[11] Sen, Amartya. *Development As Freedom*. Oxford: Oxford University Press, 1999.

[12] Morris, N. (2003) "A Comparative Analysis of the Diffusion and Participatory Models in Development Communication." *Communication Theory*, 13: 225–248.

[13] Berkman Center for Internet and Society, "Technologies of Choice? – ICTs, development and the capabilities approach." May 28, 2013. Accessed Jun. 26, 2013. https://cyber.law.harvard.edu/events/luncheon/2013/05/kleine.

[14] Nyst, Carly. "Privacy in the developing world: a global research agenda." Privacy International, July 14, 2012. Accessed Jan 6, 2013. https://www.privacyinternational.org/blog/privacy-in-the-developing-world-a-global-research-agenda.

[15] Nyst, Carly. "Privacy in the developing world: a global research agenda."

[16] *OECD Guidelines for the Security of Information Systems and Networks*. Paris, France: OECD Publications, 2002. www.oecd.org/internet/ieconomy/15582260.pdf. p. 9

[17] Rodriguez, Katitza. "Surveillance Camp IV: Disproportionate State Surveillance - A Violation of Privacy." Electronic Frontier Foundation. Feb. 13, 2013. Accessed Jun 4, 2013. https://www.eff.org/deeplinks/2013/02/disproportionate-state-surveillance-violation-privacy.

[18] Government and regulatory bodies such as the European Commission and Federal Trade Commission are continuing to devote resources to mobile privacy issues. The FTC, for example, has recently released mobile privacy guidelines, while NTIA is holding a multistakeholder mobile privacy process.

[19] Bates-Eamer, Nicole, Barry Carin, Min Ha Lee and Wonhyuk Lim, with Mukesh Kapila. "Post-2015 Development Agenda: Goals, Targets and Indicators." Centre for International Governance Innovation and the Korea Development Institute, 2012. Accessed Apr. 1, 2013. http://www.cigionline.org/sites/default/files/MDG_Post_2015v3.pdf.

[20] "Information and Communications for Development 2012: Maximizing Mobile." International Bank for Reconstruction and Development / The World Bank. Accessed May 1, 2013. http://go.worldbank.org/0J2CTQTYP0.

[21] Aker, Jenny C. and Mbiti, Isaac M. "Mobile Phones and Economic Development in Africa" (June 2010). Center for Global Development Working Paper No. 211. http://ssrn.com/abstract=1629321 or http://dx.doi.org/10.2139/ssrn.1629321 p. 22

[22] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations." London: Policy Engagement Network, London School of Economics and Political Science, 2010. http://www2.lse.ac.uk/management/documents/Electronic-Health-Privacy.pdf

[23] Aker, Jenny C. and Mbiti, Isaac M. "Mobile Phones and Economic Development in Africa" (June 2010). Center for Global Development Working Paper No. 211. http://ssrn.com/abstract=1629321 or http://dx.doi.org/10.2139/ssrn.1629321 p. 22

[24] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations." p. 16

[25] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations." p. 18

[26] Sidney, Kristi, Jimmy Antony, Rashmi Rodrigues, Karthika Arumugam, et al. "Supporting patient adherence to antiretrovirals using mobile phone reminders." *AIDS Care*. 5 (2012). p. 616

[27] Talbot, David. "Big Data from Cheap Phones."

[28] Better Than Cash Alliance, "For the Development Community: Development Community Transition Success Stories." Accessed Feb. 7, 2013. http://betterthancash.org/join/for-the-development-community/.

[29] Khood, Jayadevan. "The year that was for Aadhaar, India's most ambitious technology project." Next Big What. Last modified December 18, 2012. Accessed March 7, 2013. http://www.nextbigwhat.com/aadhar-uid-impact-2012-297/.

[30] Prasad, Swati. "India unveils Aadhaar payment services ." ZD Net. Accessed Apr. 27, 2013. http://www.zdnet.com/in/india-unveils-aadhaar-payment-services-7000008660/; International Bank for Reconstruction and Development / The World Bank, "Information and Communications for Development 2012: Maximizing Mobile." Accessed May 1, 2013. http://go.worldbank.org/0J2CTQTYP0. p. 68

[31] "Saral Money Debit Cards." *The Hindu*. Dec. 13, 2012. Accessed Jan. 17, 2013. http://www.thehindu.com/todays-paper/tp-national/tp-newdelhi/saral-money-debit-cards-launched/article4194178.ece.

[32] Khood, Jayadevan. "The year that was for Aadhaar, India's most ambitious technology project."

[33] Gelb, Alan and Caroline Decker. "Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries." *Review of Policy Research* (2012) 29: 91–117.

[34] Okunoye, Adekunle . "Organizational Information Technology Infrastructure in Developing Countries." (2003). tucs.fi/publications/attachment.php?fname=jOkunoye03a.pdf. The disparity in the availability of information technology (IT) infrastructure between Western industrialized countries of the North and the developing countries of the South has long been recognized by various agencies, like The World Bank; United Nation Development Programme (UNDP); Canadian International Development Agency (CIDA); Swedish International Development Agency (SIDA), and more.

[35] Blumenstock, Joshua. "Essays on the Economic Impacts of Mobile Phones in Sub-Saharan Africa." 2012. Accessed Mar. 1, 2013. http://www.jblumenstock.com/files/papers/jblumenstock_dissertation.pdf. p. 81

[36] Kumar, Manoj. "India risks backlash hurrying through Aadhaar project." *Reuters*. Oct 25, 2012. Accessed Jan. 27, 2013. http://in.reuters.com/article/2012/10/25/india-welfare-uid-aadhaar-system-idINDEE89O04Y20121025.

[37] "Information and Communications for Development 2012: Maximizing Mobile." International Bank for Reconstruction and Development / The World Bank,.

[38] "Humanitarianism in the Network Age." UN Office for the Coordination of Humanitarian Affairs (OCHA). Accessed Apr. 6, 2013. https://ochanet.unocha.org/p/Documents/WEB Humanitarianism in the Network Age vF single.pdf. p. 40.

[39] Ahmed, Mohamed. "Threats to Mobile Phone Users' Privacy." Office of the Privacy Commissioner of Canada, Mar. 2009. Accessed Mar. 6, 2013. http://www.engr.mun.ca/~mhahmed/privacy/mobile_phone_privacy_report.pdf. p. 13-14

[30] "India: New Monitoring System Threatens Rights." Human Rights Watch, Jun. 7, 2013. Accessed Jul. 3, 2013. http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.

[41] Duggal, Pavan. "Central Monitoring System - A legal viewpoint." *The Deccan Herald*, Jun. 30, 2013. Accessed Jul. 3, 2013. http://www.deccanherald.com/content/341759/central -monitoring-system-legal-viewpoint.html

[42] "India: New Monitoring System Threatens Rights." Human Rights Watch.

[43] Eagle, Nathan, and Alex Pentland. "Reality Mining: Sensing Complex Social Systems." *Personal and Ubiquitous Computing*. no. 4 (2006). http://realitycommons.media.mit.edu/download.php?file=pdfs/realitymining.pdf. Accessed Jan. 27, 2013.

[44] Blumenstock, Joshua. "Essays on the Economic Impacts of Mobile Phones in Sub-Saharan Africa." p. 65

[45] Blumenstock, Joshua. "Essays on the Economic Impacts of Mobile Phones in Sub-Saharan Africa." p. 68

[46] Solove, Daniel. "Introduction: Privacy Self-Management and the Consent Dilemma," 126 *Harvard Law Review* (2013) p. 1879-1903

[47] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations." p. 14

[48] Burrell, Jenna. "Evaluating Shared Access: social equality and the circulation of mobile phones in rural Uganda." *Journal of Computer-Mediated Communication*, 2010 15(2): 230-250. p.236.

[49] Burrell, Jenna. "Evaluating Shared Access: social equality and the circulation of mobile phones in rural Uganda." p.236.

[50] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations." p. 15

[51] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations." p. 5-6

[52] Kumaraguru, Ponnurangam, and Niharika Sachdeva. "Privacy in India: Attitudes and Awareness V 2.0." PreCog Research / Indraprastha Institute of Information Technology, Nov. 12, 2012. Accessed Mar. 27, 2013. http://precog.iiitd.edu.in/research/privacyindia/PI_2012_Complete_Report.pdf.

[53] "Digital Security and Press Freedom in Latin America." Center for International Media Assistance, Feb. 12, 2013. Accessed 13 Feb. 2013. http://cima.ned.org/events/upcoming-events/digital-security-and-press-freedom-latin-america.

[54] Sierra, Jorge Luis. "Digital and Mobile Security for Mexican Journalists and Bloggers." Freedom House and the International Center for Journalists, 2013. Accessed Mar. 27, 2013. http://www.freedomhouse.org/sites/default/files/Digital and Mobile Security for Mexican Journalists and Bloggers.pdf. p. I4

[55] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." The Organisation for Economic Co-operation and Development (OECD), Sept. 23, 1980. Accessed Mar. 28, 2013. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[56] "The Universal Declaration of Human Rights." United Nations (UN). Accessed Jan 28, 2013. https://www.un.org/en/documents/udhr/index.shtml

[57] "Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14." Council of Europe, Jun. 1, 2010. Accessed Jan. 28, 2013. http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

[58] Examples include the Fair Information Practice Principles (FIPPs), the NTIA multistakeholder process, and so on.

[59] Kuner, Christopher. "'You Just Don't Understand':The Current EU–U.S. Privacy Battles." *Privacy Perspectives*, Feb. 28, 2013. Accessed Mar. 28, 2013. https://www.privacyassociation.org/privacy_perspectives/post/you_just_dont_understand_the_current_eu_u.s._privacy_battles.

[60] "Reasonable Expectation of Privacy." Electronic Frontier Foundation, Accessed Jun. 1, 2013. https://ssd.eff.org/tech/mobile. https://ssd.eff.org/your-computer/govt/privacyy

[61] Solove, Daniel. "Fourth Amendment Pragmatism," 51 *Boston College Law Review* 1511-1538 (2010).

[62] Eckersley, Peter. "What Does the 'Track' in 'Do Not Track' Mean?" Electronic Frontier Foundation. Last modified Feb. 19, 2011. Accessed Mar. 28, 2013. https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean.

[63] Singer, Natasha. "Do-Not-Track Talks Could Be Running Off the Rails." *New York Times*, May 3, 2013. Accessed May 28, 2013. http://bits.blogs.nytimes.com/2013/05/03/do-not-track-talks-could-be-running-off-the-rails/

[64] "Privacy Multistakeholder Process: Mobile Application Transparency." National Telecommunications and Information Administration, Jun. 13, 2013. Accessed Jun. 14, 2013. http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[65] "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network." Federal Trade Commission, Mar. 30, 2011. Accessed Jan. 28, 2013. http://www.ftc.gov/opa/2011/03/google.shtm.

[66] Miller, Claire Cain. "Lawmakers Show Concerns About Google's New Glasses." *New York Times*, May 17, 2013. Accessed May 28, 2013. https://www.nytimes.com/2013/05/17/technology/lawmakers-pose-questions-on-google-glass.html?_r=0.

[67] Nyst, Carly. "Privacy in the developing world: a global research agenda."

[68] Nyst, Carly. "Privacy in the developing world: a global research agenda."

[69] "Best Practices: Elements of a Federal Privacy Program Version 1.0." Federal CIO Council Privacy Committee, Jun. 2010. Accessed Apr. 12, 2013. http://energy.gov/sites/prod/files/Elements of a Federal Privacy Program v1.0_June2010 Final.pdf.

[70] Canuto, Otaviano. "Mobilizing Development via Mobile Phones." World Bank Institute, Sept. 01, 2013. Accessed Jun. 28, 2013. http://blogs.worldbank.org/growth/mobilizing-development-mobile-phones.

[71] Hilbert, Martin. " Big Data for Development: From Information- to Knowledge Societies." University of Southern California - Annenberg School for Communication; United Nations ECLAC, Jan. 15 , 2013. Accessed Apr. 12, 2013. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2205145.2

[72] Vijayan, Jaikumar. "Researchers exploit cellular tech flaws to intercept phone calls." *ComputerWorld*. Accessed Aug. 13 2013. http://www.computerworld.com/s/article/9241280/Researchers_exploit_cellular_tech_flaws_to_intercept_phone_calls

© 2013 New America Foundation

This report carries a Creative Commons license, which permits non-commercial re-use of New America content when proper attribution is provided. This means you are free to copy, display and distribute New America's work, or include our content in derivative works, under the following conditions:

• Attribution. You must clearly attribute the work to the New America Foundation, and provide a link back to www.Newamerica.net.
• Noncommercial. You may not use this work for commercial purposes without explicit prior permission from New America.
• Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

For the full legal code of this Creative Commons license, please visit www.creativecommons.org.
If you have any questions about citing or re-using New America content, please contact us.

main office

1899 L Street NW
Suite 400
Washington, DC 20036
Phone 202 986 2700
Fax 202 986 3696

new america nyc

199 Lafayette Street
Suite 3B
New York, NY 10012
nyc@newamerica.net

NEW AMERICA
FOUNDATION

www.newamerica.net