SPIDER ICT4D Series no. 3 | 2010

INCREASING TRANSPARENCY & FIGHTING CORRUPTION THROUGH ICT

EMPOWERING PEOPLE & COMMUNITIES

Increasing transparency and fighting corruption through ICT

empowering people and communities

SPIDER ICT4D Series No. 3 | 2010

Authors Åke Grönlund, Rebekah Heacock & David Sasaki, Johan Hellström, Walid Al-Saqaf
Editor Cecilia Strand
Book Design Daniel Berggren
Printed by Universitetsservice US-AB, Stockholm
ISBN 978-91-85991-02-0

This publication can be downloaded from www.spidercenter.org/publications

Contents

Introduction

Cecilia Strand

Citizens must have access to public information in order for democracy to function. Lack of access to information results in a non-participatory society in which political decision-making is not democratic. Access to information concerning governance of the state allows individuals to exercise their political and civil rights in election processes; challenge or influence public policies; monitor the quality of public spending; and demand accountability. Access to information and transparency are thus prerequisites for democracy as well as a key tool in the fight against corruption.

Information and Communication Technology (ICT) can support democracy and human rights by enabling and expanding citizens' social mobilization. A better informed and active citizenry, who can put pressure on national institutions to be accountable and responsive to citizens' needs and priorities,

is a fundamental component of a functioning democracy. UN Special Rapporteur, Frank La Rue, highlighted the importance of ICT for development by stating (2010:7):

> "Access to means of communication and, in particular, to electronic communications is now seen as necessary for achieving development and, therefore, should also be considered as an economic and social right. Governments should take responsibility for facilitating and subsidizing access to electronic media to ensure equitable enjoyment of this right, to combat poverty and to achieve their development goals".

AN EMPOWERED CITIZENRY – THE BEST WAY TO FIGHT CORRUPTION

Corruption is a function of both the opportunity to request/receive bribes and the risk of detection. Corruption exists in all sectors of society. It damages a country's development by undermining faith in public institutions, increase costs for firms and discourage both foreign and domestic investments. According to Transparency International's 2009 report corruption is a growing challenge for the business sector both in the developing and industrialized countries. At the level of the individual firm, it raises transaction costs and introduces reputational risks, as well as opens up for extortion. Regardless of sector and level of transactions, corruption hampers development.

Corruption falls disproportionately on the poorer members of society and hinders them from accessing scarce services. Civil society organizations in developing countries are demanding greater transparency as a key component in fighting corruption and empowering people living in poverty. Increased transparency is often dependent on political will, and civil society around the world is actively challenging their governments to open up systems to public scrutiny. When governments do not have the capacity and/or the will to launch administrative reforms to remove the opportunities for corruption, adding external pressure on officials by increasing the risk of exposure might be a workable alternative.

External pressure involves both a revitalization of mass media and empowerment of private citizens.

The need to understand the challenges to reap the benefits
The Swedish Program for ICT in Developing Regions (SPIDER) is a national network supporting partners in developing countries in the areas of health, governance and entrepreneurship. While ICT is not a magic bullet when it comes to ensuring greater transparency and less corruption, SPIDER is convinced that it has a significant role to play as a tool in a number of important areas:

- ICT can improve transparency in the public sector by increasing the coordination, dissemination and administrative capacity of the public sectors', as well as improve service delivery by employing user-friendly administrative systems.
- ICT facilitates the collection of digital footprints and complete audit trail which increase the opportunity to hold individuals accountable and ultimately increase the possibility to detect corrupt practices.
- ICT can facilitate the work of civil society organization working towards greater transparency and against corruption by supporting a mix of methods of campaigning on transparency and educating citizens on what corruption is about and their civil rights.
- ICT can facilitate information sharing and social mobilization and ultimately provide digital platforms where citizens can report incidents anonymously.

In this issue of the ICT4D Series 2010, the potential of ICT in these areas are explored and analyzed in greater detail.

Professor Åke Grönlund's chapter, 'Using ICT to combat corruption – tools, methods and results' outline that while the eradication of corruption using ICT is dependent on several factors and difficult to achieve, it does have a real potential. Through a comprehensive analysis of relevant theories and a number of concrete cases, Professor Grönlund systematically

shows that ICT - interventions need to be launched together with real administrative reforms in order to be successful. Together with comprehensive administrative reforms ICT can decrease corruption by increasing transparency, introduce systemic hurdles, as well as increase the risk of detection.

Rebekah Heacock and David Sasaki explored the concept of ICT as a means to increase transparency in Sub-Saharan Africa in depth and highlight the growing potential by analysing a number of East African initiatives. The authors argues that while there is resistance among some governments, there are parallel to that both strong visionaries and a growing body of tech-savvy citizens willing and able to challenge that resistance. The authors also highlight the need for donors to acknowledge their part in aiding non-transparent practices and call for greater aid transparency. Lack of transparency within international development cooperation ultimately makes it difficult for citizens to hold their own governments accountable.

There are still significant challenges in realizing the potential of new technologies due to issues of access. The Internet is providing over a billion people with unprecedented access to information and communication tools, but the vast majority of the world's citizens have no or limited access to the Internet. PhD Candidate, Johan Hellström, challenges the access argument by highlighting the explosion of mobile phone access and use in his chapter 'Mobile technology as a means to fight corruption in East Africa'. In Eastern Africa there are 50 million mobile subscribers and people spend almost 50% of their disposable income on mobile communication. Hellström argues that if mobile interventions can develop beyond the pilot-study-syndrome and find solutions to privacy concerns, and develop sustainable business models; then "mobile solutions give citizens a voice, bigger ears and hopefully, a chance to mobilise and act upon the information".

The first three chapters all touch upon a crucial point – the realization of ICTs potential is dependent on the surrounding

political, social, economical and infrastructural environment. These factors will in part decide if the technology can be used to its fullest potential. ICT will thus remain unrealized in some contexts due to efforts by governments to control it. In a recent report of the UN Special Rapporteur, Frank La Rue, on the promotion and protection of the right to freedom of opinion and expression (2010, A/HRC/14/23), this development is noted with concern. Moreover, the Rapportuer highlights the following phenomena of particular concern:

1. The fragmentation of the Internet through the imposition of firewalls and filters, as well as through registration requirements;
2. State interventions, such as blocking of websites and web domains which give access to user-generated content or social networking, justified on social, historical or political grounds;
3. The fact that some corporations which provide Internet searching, access, chat, publishing or other services fail to make a sufficient effort to respect the rights of those who use their services to access the Internet without interference, for example on political grounds.

PhD Candidate Walid Al-Saqaf chapter 'Internet Censorship Challenged' analyze this very important issue, as well as, explore ways to address it through various circumvention techniques.

ICT is not a magic bullet when it comes to ensuring greater transparency and less corruption, or strengthening democracy. Nevertheless, with this issue of the ICT4D Series, SPIDER wishes to highlight the potential of ICT, and take an active part in addressing the challenges.

Using ICT to combat corruption
- tools, methods and results

Åke Grönlund

Transparency International (TI), the most cited source in corruption discussions, defines corruption as the abuse of entrusted power by political leaders or bureaucracy for personal gain or specific group interest. Most other international organizations, such as the UN and the World Bank, use either that definition or very similar ones. ICT has been identified as a viable tool for diminishing corruption by enhancing transparency and accountability of government administration. For example, the World Bank defines electronic government (eGovernment) as "the use of information and communications technologies (ICT) to improve the efficiency, effectiveness, transparency and accountability of government" and argues that "E-Government helps to increase the transparency of decision-making processes by making information accessible – publishing government debates and minutes, budgets and expenditure statements, outcomes and rationales for key

decisions, and in some cases, allowing the on-line tracking of applications on the web by the public and press" (World Bank, 2010a). By this logic ICT is supposed to help mainly indirectly. Making information public will allow audit and hence induce a change in people's behaviour.

ICT can, however, also intervene more directly. By automation of processes it is possible to significantly reduce opportunities for corruption by removing human agents at data collection and service delivery points – when people engage in e-banking there is no officer to bribe (Bhatnagar, 2003). Moreover, "anti-corruption" software tools can track various events in electronic systems that signal not only illegitimite actions that have already taken place but also proactively detect suspicious behaviour before any crime has been committed. This may serve as a real deterrent as well as a monitoring tool. Such systems can, to some extent, assist in tracking anomalies in operations, in observing systematic features of customers' reporting about errors or misuse, and in social media analysis (Gilliatt, 2007).

This article investigates the current state of the art by discussing the following questions:

- What is corruption?
- How is ICT supposed to help reducing corruption?
- What is the evidence of ICT's role so far?

Based on the findings the paper concludes by discussing various proposals for ways forward.

WHAT IS CORRUPTION?

As noted above, Transparency International (TI) defines corruption as the abuse of entrusted power by political leaders or a bureaucracy for personal gain or specific group interest. The UN points out that corruption can take many forms that vary in degree, from the minor use of influence to institutionalized

bribery, and that "this can mean not only financial gain but also non-financial advantages" (UN, 2010). In this context it should also be noted that it can take place in both online and offline environments, and that even if it takes place offline – which no doubt most corruption does – it may leave traces online such as interpersonal communications, money transfer, and indeed the opposite – lack of transactions. Further, wherever corruption takes place, one locus for combating it is online, as the Internet is increasingly the forum for achieving transparency, awareness raising and debate.

Defining corruption is one thing, measuring it is a different matter. Being an undercover activity, corruption usually leaves no direct trails in paper or computerized records. Hence, information needs to be collected by other means. One of these is engaging the public: "Responses about corruption based on individuals' actual experiences are sometimes the best available, and the only, information we have" (Kaufmann, Kraay and Mastruzzi, 2006). The public can be enlisted in several ways. At the micro level – projects and specific service processes – there are guidelines for what is allowed and what is not, how to detect corruption, and how to prevent it, e.g., by managing projects meticulously (e.g. UNDP, 2004; Olsen, 2010).

At the macro level (national) there are several indices developed for corruption measurement (UN, 2008). Two commonly used ones are TI's Corruption Perceptions Index (CPI) and the World Bank's Corruption Control Index (CCI). Measuring corruption is inherently difficult as it is largely an undocumented activity. Therefore, what is measured by the various indices is largely a number of proxy variables. CPI measures the level of corruption in countries based on experts' perceptions. CPI focuses on petty corruption, bribery in government services-to-citizens operations. It uses data from fourteen sources from twelve independent institutions. All sources measure the overall extent of corruption (frequency and/or size of bribes) in the public and political sectors and all sources provide a ranking of countries (UN, 2008).

The CCI is used for annual evaluations as well as being a measure used in research (Kaufmann et al., 2003; Lindstedt, 2005:22f). Compared to the CPI, the CCI draws on more data as it comprises 195 countries and also includes data collected from citizens (Kaufmann et al., 2007:75).

Focusing on larger-scale corruption, the Bribe-Payers' Index by TI ranks 30 leading exporting countries according to the propensity of firms headquartered in those countries to bribe when operating abroad. This is an indirect measure of the soil for corruption in a country. More direct measures include the World Bank CPIA (Country Policy and Institutional Assessment) index which measures the quality of policy and institutional environments by a large set of criteria, including the regulatory environment, policy and institutions, rule-based governments and more (UN, 2008; World Bank, 2010b).

The Global Integrity Index (Global Integrity, 2006) measures corruption in terms of its opposite, i.e., factors that contribute to reducing corruption; the existence, effectiveness of, and the citizen access to key anti-corruption mechanisms at the national level in a country. Like the CPIA it measures institutions rather than corruption per se.

This brief and certainly not complete review has been pursued to make the point that there are many different indices with different foci; petty as well as large-scale corruption, micro (project) as well as macro (national) level, symptomatic (measuring corruption-related activities) or systemic (measuring the quality of institutions). Measuring is important for understanding, but even though measurement is incomplete there is at least a certain level of understanding of a number of factors that in different ways entail, facilitate, or fail to prevent corruption. There is a need to take some action. This is where ICT comes in; how can it address at least some of the factors known to be conducive to corruption? Beyond the definition of terms, several studies have attempted to unravel what causes corruption. A commonly used causal model, first introduced by Robert Klitgaard (1998), proposes that it is a

problem of asymmetric information and incentives. Klitgaard draws on the commonly used principal-agent-client model; each actor can have different interests and the agent is under some circumstances both empowered and inclined to act for his own purposes rather than those of his principal and his principal's client. Klitgaard claims that corruption occurs when a public official can operate in a situation of information monopoly, can administer an operation in discretion, and a lack of accountability. The formula reads, Corruption = Monopoly+ Discretion-Accountability. Transparency International (TI) adds a community factor, called ethical ambience, to the equation. This refers to "the sense of community, of responsibility for the common good and of ethics" (Moor, 1998). The ensuing extended TI definition reads Corruption = (Monopoly+ Discretion-Accountability) / Ethical ambience (TI, 2004:14).

The obvious, however difficult, ambition then includes to dismantle monopolies, avoid discretion, and increase accountability and the positive ethical ambience. Here, ICT stands out as a useful tool as it can address at least some of these factors.

THEORY – HOW CAN ICT HELP?

Monopolies and discretion are corruption facilitators, while accountability and an anti-corruption ethical ambience in communities are inhibiting factors. There are several ways in which ICT can contribute positively to changes regarding these factors.

Monopolies

The process of constructing electronic services entails transferring information held by government agencies, or individual civil servants, into electronic platforms and presenting it to users in forms defined by laws and process regulations by means of linking different databases. Because this is done automatically there is no room for individuals to exert influence by manipulating or withholding information as long as

the user has direct access to the electronic service; automation removes the agent. Using electronic services also means introducing competition by providing alternative delivery channels . This way users can choose to avoid agents who are corrupt (Bhatnagar, 2001). However, there may still be local monopolies in providing the e-services, for example in telecentres or e-kiosks, and there are services where there are "natural monopolies", such as tax administration and customs; two sectors from which incidentally there are typically reports of high risk for bribery and for which e-services are claimed to be most beneficial.

Dismantling of monopolies (governmental or outsourced) requires administrative reform (Bhatnagar, 2001a; Hanna, 2004). Rumel (2004) claims that, to be effective, such reforms require at least a minimum of democratic governance. Kettl (2000:33) states that "Experience demonstrates quite clearly that tactics such as outsourcing, customer service, and information technology do not – and cannot – manage themselves. Indeed, they require aggressive and thoughtful oversight." It has been suggested that ICT is no substitute for poor management. While obviously management matters, the very process of building an on-line delivery system requires that rules and procedures are standardized across regions and made explicit so as to make them amenable for coding which reduces the discretion on part of civil servants and increases the auditability of operations (Bhatnagar, 2001a; Lau, 2001). This means that eGovernment itself can be used as a starting point for reengineering processes and making them less corruption prone.

Discretion

The very idea of electronic services is that the user interacts with an electronic system where rules are strictly specified, rather than with a civil servant. While the main reason for electronic services is typically related to cost savings, clearly automation removes the possibility of the civil servant acting on his or her personal discretion. Rumel (2004) calls this process of taking the agent out of the principal-agent model

"disintermediation", which means that the client interacts directly with the principal by means of the rules implemented in the IT system; strictly, so that the computer follows rules without discretion. Wherever the user has direct access to an electronic service, the opportunity for the civil servant at the particular point of computerization to refuse a service unless paid personally is removed.

However, it may shift the exercise of discretion to other places in the service process. First, there may still be some person guarding access, in particular when clients are illiterate or do not have access to a computer and hence may not be able to use the service directly themselves. Provision of services at telecentres may serve as at least a partial safeguard against this risk, as in such settings there are many people around serving as witnesses which provides openness to the situation, which in itself is a barrier towards corruption. Second, even though the front end of a service is computerized, there may be manual handling in the back office where civil servants may find room for discretion. Finally, there may be discretion involved in implementing and maintaining the computer systems (Reddick, 2005). Computerization projects as well as outsourcing service contracts may be targets for bribes. Some claim that this way ICT may even provide an opportunity for more corruption (Heeks, 1998).

Accountability

Accountability refers to the "service guarantee" of a government; the extent to which its actions are accounted for and corrected if not carried out correctly in the first instance. Technically, accountability can be improved fairly easily. Information can be published online, processes and decisions can be traced for audit and analysis, and there can be rules for compensation where accountability is not delivered. For this to happen, however, there is a need for a set of firm laws regarding government procedures in general and how they should be handled in the IT medium in particular. In recent years all countries have needed to update their laws to cater for accountability in electronic services, but comprehensive

and effective legislation is not yet at hand in many countries. It requires openness of processes, access by the public, transparency of rules, processes for complaints handling, etc. There are studies showing that the greater the access to information, the lower the corruption levels (DiRienzo et al., 2007).

Community/Ethical ambience

Many international organizations provide "anti-corruption toolkits", both general ones and those targeted towards different audiences, such as politicians, local communities, local government, project managers, youth, specific countries or regions, businesses, etc. The toolkits are overall similar in content. They include codes of ethics for professionals, conflict of interests laws, whistleblower protection, ethics training, etc. Examples include the UNESCO UN Anti-Corruption Tool Kit (UNESCO, 2007), Transparency International's anti-corruption education (TI, 2010), the World Bank resource centre (World Bank, 2007), and the anti-corruption toolkit at the website: anticorruption.org (2000). Over the past few years ICT has become increasingly important in this field due to the phenomenon of the "social web". Organizations increasingly try to use various online forums to promote ethical behaviour.

Table 1 summarizes what kinds of corruption ICT can – in principle – help combat, and how. In most cases, at least when petty cash corruption is concerned, there is no need for high-tech solutions, standard technologies will go a long way. Bhatnagar (2003 and 2009) provides numerous examples of where transparency based on automation and reporting has managed to go quite some way. High-stake corruption is different in locus as well as procedures and more advanced ICT tools may be of assistance.

ICT tools for corruption combat

There are numerous ICT tools that can be used during various phases of combatting corruption, including prevention, detection, analysis, and corrective action.

Table 1: Summary of ICT based actions to combat corruption

Action type	Logic to achieve benefits	Main target	ICT used
Automation	Remove human agents and hence corruption opportunities from operations	Petty bribery in everyday operations	Any system
Transparency	Remove opportunity for discretion	Mobilize the public, inform users	Web sites where information is published. Manual or automatic input
Detection in operations	Both details and aggregates from operations can be monitored to detect anomalies and unexpected performance	Petty bribery as well as large-scale operations	Log analysis tools, standard as well as specifically targeted ones Control functions in e.g. procurement systems
Preventive detection	Online social networks and individuals can be monitored to detect preparations for corrupt action	Large-scale corruption, e.g. in procurement or international trade	Social network analysis and social media analysis tools
Awareness raising	If the public is aware of government rules and procedures they are better able to resist arbitrary treatment	Petty bribery	Any techniology, but web sites are most common
Reporting	Mobilizing users/community to report cases will make it easier to take corrective action towards individuals and to reorganize systems to avoid "loopholes"	Petty bribery Large-scale operations	Web sites, social media networks, online newspapers, mobile phones, SMS for input
Deterrence	Publishing information about reported corruption as well as indicators (such as imbalance between income and property) will deter civil servants from engaging in corruption.	Petty bribery	Web sites, social media networks
Promoting ethical attitudes	Engaging the public by means of pursuing discussions in various online forums	Public attitude change	Social media forums

Anti-corruption software is a label used for various tools designed specifically for detecting and taking action against fraud, including both "intelligent mining" of data sets and administrative procedures. The origin of the tools can be traced to methods used for intelligence and police work. For example, the "Pursuit" software from Distillery Software (http://www.distillerysoftware.com/industries/anti_corruption.html) contains tools for intelligence "allowing investigators to capture rich entity and association data and build up a picture of relationships between persons of interest, assets, events and organisations", complaints management and investigation management. Complaints and investigations management are basically administrative tools facilitating various proce-

dures involved, such as "Witness and Exhibit Management" (management of structured and unstructured data), "Brief of Evidence/Case File Production" (produces court documents automatically as output from the other tools), and "Asset Tracking" (linking to individuals and organisations, and tracking actions in relations to those assets). These are tools focusing mainly on systematic and/or large-stake corruption and they operate only in the electronic world so things that take place exclusively in the physical world escape attention. However, small-stake corruption can also be traced this way. For example, one of the effects of even petty corruption is that civil servants own more expensive property than they can reasonable afford given their official salary, and asset tracking is one way of systematically finding this out. Another way to do this is, of course, by coordinating existing government records of people and properties, if such exist sufficiently.

Such software is reportedly used by the Kenya Anti-Corruption Commission (Kenya Anti-Corruption Commission, 2010), but similar software functionality, developed in-house or off-the-shelf, is used also in other countries – and for other purposes, which is a particular point of concern. No doubt corruption fighting is important, but monitoring people's actions may also conflict with human rights and privacy legislation (in countries where such exist) and concerns (in all countries). The tools can be used to trace not just corruption but also terrorism, refugee communities, and any activity, not just illegal ones.

Social Network Analysis (SNA) software are general tools to analyse communication patterns on the Internet. While some of the functions are similar to anti-corruption software this group of tools has an entirely different background. They stem from market research and most aim to provide companies with tools to chart, understand, and communicate strategically with their customers. The underlying "intelligence" in the systems comes basically from two strands of research; social network analysis and linguistics.

Social network analysis techniques can detect various characteristics of networks, in this case of people communicating on the Internet. Examples of such analyses include (but are not limited to) detection of cohesive subgroups (cliques, clans) and regions (components, cores), centrality analysis, network density, distances, detection of structural holes. These are technical terms describing network composition, which in simple terms basically identify who is the leader of a group, who are his/her executives/closest associates, and who are the followers.

If this information is coupled to other information, historical as well as present, about specific people, such as their assets or their relation to companies that take part in public procurement processes where corruption may occur, it is possible to trace not just illegal actions but also preparations for such, in particular when combined with the use of linguistic tools. Beyond the available commercial software there is also the obvious option for any country to invest in in-house development and build proprietary software that contains functionality designed to help fight corruption in ways specifically designed to meet local conditions.

Two examples are found in India and Russia:

In India, the National Rural Employment Guarantee Act (NREGA) guarantees wage employment to every household whose adult members volunteer to work on labour-intensive public works annually. The system is administered in a way that even its proponents admit holds ample opportunity for corruption and further exploitation of the rural poor it intends to serve. An investigation has found that officials and politicians inflate work bills, fake wages and pocket funds. To bypass the human agents involved in the administrative process, computers, not officials, now issue job cards, provide work estimates, and generate each worker's pay slip online (at www.nrega.ap.gov.in). Payments are made into individual postal accounts created for the purpose. Reportedly this technologically uncomplicated measure has so far recovered

a substantial amount of misappropriated funds (Srivastava, 2008).

In Russia, an attempt to fight corruption in government procurement by including automatic checks in the process was announced as "Dmitry Medvedev's Anti-Corruption Software. President Puts the Fight against the Main Evil into Automatic Mode" (Sergeev, 2008). The official website of governmental procurements will automatically detect signs of corruption in the bids submitted by government agencies and state-owned enterprises. The Federal Antimonopoly Service will be notified automatically of improperly composed bids. Checks include various formalities as well as loopholes created in translation between Cyrillic and Latin alphabets. Reportedly the software detected 190 bids with suspicious distortions in a single week. However, many believe that information control over governmental procurements will be ineffective as subsequent extortion will remain. "In the late 90s [the] share of kickbacks in public procurement was estimated at 10–15%, but today – despite the use of Internet technologies – it has grown significantly" (ibid).

HOW HAS ICT PERFORMED IN REDUCING CORRUPTION IN PRACTICE?

The effects of ICT/electronic services/electronic government and community on corruption have been studied at micro (project) level as well as macro (national) level.

Macro level studies (nations)

Andersen (2009) estimated the impact of eGovernment on corruption using the changes in the CCI index from 1996 to 2006 and found that different countries' eGovernment maturity development (as measured by the index of West et al. (2006) was reflected in positive change of CCI, and quite strongly so. When a country implements more eGovernment there follows a considerable reduction in corruption. Andersen also tested the effect of the variables of GDP per capita and

the degree of "free press". The study found that the growth rate of GDP per capita is always significant, whereas a free press did not seem to influence changes in corruption.

Shim and Eom (2009) examined how the two factors social capital (the strength of positive social relations) and ICT affected corruption and found that both factors individually had positive effects on corruption. Shim and Eom measured corruption by the TI Corruption Perception Index (CPI). ICT was measured by three factors, (i) the UN eGovernment readiness index, (ii) the UN e-participation index, and (iii) internet penetration. The measure used for social capital was the World Value Survey (WVS), an international research project that measures the values held by people from around the world. ICT had positive effects on corruption, and social capital had anticorruption effects independently of ICT. The authors conclude that "policies designed to foster trust networks in a society can contribute to the reduction of corruption". As for the impact of ICT on corruption, e-readiness and e-participation were significant. Controlling for bureaucratic quality, rule of law, anti-favouritism, and competence of government officials, the ICT variables were still statistically significant. They found that the three ICT variables accounted for 77 % of the total variation of corruption, which means that ICT variables had a substantial effect. In fact, ICT variables were more influential in terms of reducing corruption than traditional anti-corruption factors. The authors conclude that "in addition to the traditional anti-corruption approaches, i.e. administrative reform and law enforcement, ICT could be an effective tool in reducing corruption". These studies combined suggest that the often stated assertion that administrative reform must come first and ICT only later does not hold true. ICT reform also drives administrative reform. ICT can hence be a good place to start.

Micro level studies (projects)

Many studies of ICT in developing countries concern India, as that country has invested massively in various electronic services from government as well as distribution systems such

as kiosks, "eSevas" and telecentres. Two major projects which have been much studied both for their ambition and outcome and for their particular focus on curtailing corruption are Bhoomi and CARD. They are interesting because although similar in design the outcome turned out very differently.

Bhoomi

The Bhoomi project was initiated in Karnataka by the Department of Revenue (DoR). The project was designed to facilitate online delivery of land records so that citizens could challenge arbitrary bureaucratic action if they deemed them to be unfair. It was also designed to automate the internal government processes to remove discretion from civil servants (Chawla and Bhatnagar, 2001). In terms of the size of its operation, the project has been succesful. Since inception the project has computerized 20 million records for 6.7 million farmers. Before the implementation of Bhoomi, farmers were required to seek assistance from the Village Accountants (VAs) in order to obtain a copy of their 'Records of Rights, Tenancy of Crops' (RTCs). These documents are requisite for farmers to apply for bank loans (Bhatnagar, 2002). Traditionally, the time taken to obtain RTCs ranged from 3 to 30 days depending on the type of document and where it was obtained. If farmers decided to purchase or sell farm land, mutation requests were to be filed with the help of VAs. The VA posted the information at the local office for interested parties. If there were no objections within 30 days, land records were updated in the presence of the revenue inspector (RI). The VAs were also collecting bribes and forwarding them up the bureaucracy. The amount of bribes depended on the importance of the documents. A typical bribe in 2002 ranged from US$2 to US$40 (Bhatnagar, 2002:26).

The Bhoomi project was hence in practice "disintermediating" the service (Rumel, 2004). Automating the mutation requests removed the citizens' need to deal with VAs, which was also the point of corruption in the previous system. Nine thousand VAs were replaced or bypassed because farmers could now obtain a printed copy of the RTC at 800 kiosks (in 2009) in

Karnataka as well as check the status of their mutation request. The operators of the information system had to log in via thumb print authentication which eliminates the possibility of password fraud. This measure was designed to avoid discrepancies so that the corrupt behaviour could be detected easily.

Although the central role of the VAs was replaced by computers, the role of the RIs, another point of corruption, still remained as before (Bhatnagar, 2003). A World Bank evaluation report concludes that "Corruption and harassment in some government practices have decreased a bit. Most people perceive a lowering of corruption and less harassment, at least for some of the public services that are available through Gyandoot like income/caste/domicile certificates. The impact is minimal, but people feel that something is changing" (Arazyan, 2002).

The project has taken measures to increase government accountability by installing a system of electronic grievances, and the handling of these is followed up to see if they are responded to. However, the system still has holes in the verification chain, as the Bhoomi is not connected electronically to the Registration Department: "Village accountants working in the field are apparently still getting bribes for work on mutations" (Arazyan, 2002).

Some studies have claimed that Bhoomi reduced corruption from 66 % to less than 3 % (Pathank and Prasad, 2006; Bhatnagar, 2003). A 2006 study suggest the reduction is from 29.7 % to 0.8 % for RTCs and from 33.8 % to 0.7 % for mutations (Bhatnagar, 2009). While all these numbers appear impressive they also point to the difficulty of measuring corruption. Input data is people's self-reported frequency of paying bribes. This data may not be accurate as people may have forgotten with the lapse of time, possibly years, since they used the manual services, which probably is one explanation for the great variation in the "before" numbers between the different studies (ranging from 30 % to 66 %), and which means that

the "after" numbers should also be used with caution. According to Bhatnagar (Personal communication via email, 9 May 2010), the sample and sampling methodology was also more rigorous in the recent studies as compared to the earlier 2002 study.

While evaluations are not conclusive it seems clear that the Bhoomi project has had considerable success in addressing the Discretion and Accountability parts of the corruption equation (C=(M+D-A)/E). However, there are still loopholes, and without tender care, local monopolies will be created or sustained. "There is no substitute for good management" (Bhatnagar, 2003).

CARD

The Computer-aided Administration of Registration Department (CARD), is a property registration system implemented in the state of Andhra Pradesh (AP) by the Registration Department (RD). The goal was to increase transparency and efficiency in the land registration process and ultimately reduce corruption. CARD assists officials in the sub-registrar office (SROs) complete the property registration procedure. The registration process consists of four steps; purchasing paper bearing an official stamp, establishing price of the property, determination of the applicable duty, and recording of the details of the transaction (Prakash and De, 2007). Before the introduction of CARD, the RD was severely corruption-ridden. The staff at the entry point of the registration process (printing and filling out forms) demanded bribes before the registration forms could be moved through the process. Once the forms were processed at the entry point, mid- and senior level staff with authority to complete registration and other services could demand bribes at any point.

The CARD system can be used to assess property value, enter data and prepare sale deeds. The system allows searching for encumbrance, certification, and certified copies of documents. The system registers 1.18 million documents per year and serves 5 million citizens. Although some portion of the reg-

istration process was computerized, the registration process could not be automated because existing laws such as the 1899 Stamp Act and the 1908 Registration Act were not adopted for the effectiveness of the CARD. However, several other statutes were amended, mainly to recognize digital records and computer printouts as legal documents.

Although paper forms were replaced with computer printouts and the paper records were changed to digital format, the officials still enjoy a monopoly over printing stamped papers (using computers), revenue collection, and stamp duties. Even though the registration was partly computerized, nothing changed for citizens because they were still required to bribe from the starting point of the registration process all the way until the registration was completed. "Even though the CARD was designed to reduce corruption, the civil servants did not allow its functionality to be integrated because of heavy resistance from the corrupt officials" (Caseley, 2004). The project did not meet the original objective of reducing corruption because the project did not have support from the department head or politicians (Casely, 2004). However, the project has improved the possibility for inspection. With CARD, civil servants have information at their fingertips and can search for information very quickly (De, 2007:5).

The Bhoomi project was designed to combat corruption and it was implemented effectively. The department head was able to deliver strong leadership and acquire political support. In the case of CARD, leadership was less successful. Although some literature suggests CARD was able to eliminate middlemen and organized corruption, thus reducing corruption by 90% (Pathak and Prasad, 2006), there is other evidence. Bhatnagar (2009) reports that the practice of bribing was only reduced marginally, from 28 % to 24 %. Given the uncertainty in the data used, this reduction is hardly significant.

It should be noted that CARD has been evaluated positively by other measures, mainly by reducing waiting and travelling times for citizens (Bhatnagar, 2007).

From the examples of Bhoomi and CARD one can conclude that management matters, and greatly so. It is typically assumed that implementation of e-government systems minimizes corruption in developing countries. However, as Dé (2007) finds, the existing conditions in which e-government systems are introduced as well as the inherent design of the systems will determine their effect on corruption, something of which the Bhoomi and CARD cases are evidence. eGovernment systems must increase access to information, ensure that rules are transparent and that they are applied in specific decisions, and build the ability to trace decisions/actions to individual civil servants (Bhatnagar, 2002). When all these objectives are pursued at the same time, corruption can be reduced significantly, but ignoring some of them can defeat the purpose altogether. Combatting corruption requires adminstrative reform; it is not a straightforward ICT matter. Corruption is rooted in the cultural, political, and economic circumstances of those involved. ICT does little to affect these root causes. At the national level, one needs political will, ethical watchdog agencies, proper incentives for honest officials, and effective punishment for corrupt ones (Quah, 1999). Bhoomi succeded impressively, even interpreting the evaluations conservatively; CARD did not.

DISCUSSION AND CONCLUSION

Although there is a scarcity of reliable data, there is at least some evidence that ICT can be an effective tool to combat corruption. The potential of ICT can, however, only be realized when it is combined with real administrative reforms. One of the positive findings is that ICT also drives such reform. The article has studied corruption at two distinct levels, national and project/process. Regarding the national level, three findings have been presented.

- More eGovernment is better; the more services online in a country, the less corruption. The effect is considerable (Andersen, 2009).

- ICT has a greater positive effect than the traditional anti-corruption factors (e.g. administrative reform without the development of technological support systems, free press) (Shim and Eom, 2009; Andersen, 2009).
- Increased social capital (stronger social bonds) reduces corruption (Shim and Eom, 2009).
- This means that even though clearly several individual projects are not successful, the overall balance is positive – ICT investment in eGovernment pays off in terms of reduced corruption. One possible limitation in these studies is their dependency on the quality of the indices used. More research is needed to investigate how robust these measurements are across different indices.

At the project level there are a number of factors determining what makes projects succeed or fail from a corruption perspective.

- Management matters. A major difference between the Bhoomi and CARD projects is the different leadership and their focus on corruption reduction.
- Administrative reform must focus on whole systems, not just individual functions. Wherever there is a loophole due to some technical component missing there is an opening for corruption. This was seen in failed projects as well as in successful ones. The latter had fewer loopholes because of a more systematic design (e.g. Bhoomi).
- Corruption is an economic activity. When bribes are cheaper than fees there is a market for corruption, when fees are lower than bribes there are good chances of reducing it, as was shown in the Bhoomi case.
- Political support makes a difference. It contributed to the success of Bhoomi, and the lack of it contributed to the failure of CARD (regarding the corruption effect).
- Creating an "ethical ambience" among the public requires trustworthy reporting systems and prompt corrective action from government.

This paper has shown that ICT can indeed bring a positive difference but only in combination with skilful and determined use. Beyond the specific findings listed above, there are developments that are still in their infancy and require more research.

Advanced tools for "social network analysis" are potentially very useful but these tools require a considerable amount of skill and care in use so as to avoid over interpretation and the pursuit of innocent people, hence violating human rights with all its consequences not just for individuals but also for states and companies. So far these tools have mainly been used for national intelligence, and the migration into more "civil" activities is not straightforward. More research is needed not just on how these tools can be effectively used but also how they can be ethically used.

The use of "social software" or "web 2.0 tools" to promote ethical attitudes requires considerable human resources. There is also a question as to just how much government itself should engage in such activities, for reasons of credibility as well as of resources and policy. There is as yet no clear answer to this question as the role of government in social media is currently at an experimental stage.

REFERENCES

Andersen, T.B. (2009) 'E-Government as an anti-corruption strategy'. *Information Economics and Policy*. 1:3, pp 201-210.

Anticorruption.org (2000) *Anti-corruption toolkit*.
Available online at: http://www.anticorruption.bg/index.php?id=803, retrieved 22 April 2010.

Arazyan, Hmayak (2002) 'Evaluation of Gyandoot and Bhoomi (India). An interview with Simone Cecchini, research analyst with the Poverty Reduction Group, Poverty Reduction and Economic Management, The World Bank'.
Available online at: The Development Gateway. http://topics.developmentgateway.org/search/Search-results.do?in_desc=true&in_title=true&searchString=cecchini, retrieved 15 September 2010

Bhatnagar, S. (2001a) 'Administrative corruption: How does E-government help?'
Available online at: http://www1.worldbank.org/publicsector/egov/transparency.htm.

Bhatnagar, S. (2001b) 'Central Vigilance Commission website: A bold anticorruption experiment'.
Available online at: http://web.worldbank.org/wbsite/external/topics/extinformationandcommunicationandtechnologies/extegovernment/0,,contentmdk:20485999~menupk:1767268~pagepk:210058~pipk:210062~thesitepk:702586,00.html, retrieved 15 September 2010

Bhatnagar, S. (2003). Transparency and Corruption: Does E-Government Help? DRAFT Paper prepared for the compilation of CHRI 2003 Report *Open Sesame: looking for the Right to Information in the Commonwealth*, Commonwealth Human Rights Initiative, 2003.
Available onine at: http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan035963.pdf, retrieved 15 September 2010

Bhatnagar, S. (2009) *Unlocking E-Government Potential. Concepts*, Cases and Practical Insights. Sage Publications India.

Chawla, R. and Bhatnagar, S. (2001) 'Bhoomi: Online delivery of land titles in Karnataka, India'. World Bank.
Available online at: http://info.worldbank.org/etools/docs/reducingpoverty/case/96/fullcase/India%20Bhoomi%20Full%20Case.pdf, retrieved 15 September 2010

DiRienzo, C.E., Das, J., Cort, K.T., and Burbridge, J. (2007) 'Corruption and the role of information', *Journal of International Business Studies*, Palgrave Macmillan Journals, 38(2), pp 320-332

Gilliatt, N. (2007) 'The usual list'. 27 March, 2007.
Available online at: http://net-savvy.com/executive/social-media-analysis/the-usual-list.html, retrieved 15 September 2010

Global Integrity (2006) The Global Integrity Index 2006.
http://www.globalintegrity.org/data/2006index.cfm

Kaufmann, D., Kraay, A., and Mastruzzi, M. (2003) *CCI: Governance Matters III: Governance Indicators for 1996-2002*. World Bank Policy Research Working Paper No. 3106, 30 June, 2003.

Kaufmann, D., Kraay, A., and Mastruzzi, M. (2007) *Governance Matters VI: Governance Indicators for 1996-2006*. World Bank Policy Research Working Paper No. 4280.
Available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=999979, retrieved 15 September 2010

Kenya Anti-Corruption Commission (2010) Available online at: http://www.kacc.go.ke/default.asp?pageid=16

Lau, E. (2001) 'E-government and drive for growth and equity'. Organization for Economic Cooperation and Development E-Government Project.
Available online at: http://belfercenter.ksg.harvard.edu/files/lau-wp.pdf, retrieved 15 September 2010

Moor, Jay (1998) 'On good behaviour: Corruption and ethics', in *Habitat Debate*, Vol. 4, No. 4, UN-HABITAT, Nairobi, p. 24.

Olsen, William P. (2010) *The Anti-Corruption Handbook: How to Protect Your Business in the Global Marketplace*. Wiley.

Pang, Bo and Lee, Lillian (2008) 'Opinion Mining and Sentiment Analysis', *Foundations and Trends® in Information Retrieval*. 2(1–2), pp 1-135.
Available online at: http://dx.doi.org/10.1561/1500000011, retrieved 15 September 2010

Park, Hun Myoung (2005) 'A cost-benefit analysis of the Seoul OPEN System: Policy lessons for electronic government projects', HICSS, vol. 5, *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (HICSS'05) p.126b,

Prakash, A., and De', R (2007) 'Importance of development context in ICT4D projects: A study of computerization of land records in India'. *IT & People*, 20(3): 262-281.

Rumel, Mahmood (2004) 'Can information and communication technology help reduce corruption? How so and why not: Two case studies from South Asia'. *Perspectives on Global Development and Technology*, 3(3): 347-373.

Reddick, C.G. (2005) 'Citizen interaction with E-Government: From the streets to servers?' *Government Information Quarterly*, 22(1), 38-57.

Sergeev, M. (2009) 'Dmitry Medvedev's anti-corruption software. president puts the fight against the main evil into automatic mode'. *Nezavisimaya Gazeta* 209-10-09.
Available online at: http://www.ng.ru/economics/2009-10-09/1_soft.html?mthree=1, retrieved 15 September 2010

Shim, D.C., and Eom, T.H. (2009) 'Anticorruption effects of information communication and technology (ICT) and social capital'. *International Review of Administrative Sciences*, 75 (1): 99-116.

Srivastava, P. (2008) 'A new software that keeps politicians as honest as possible'. *Think Change India*.
Available online at: http://www.thinkchangeindia.org/2008/04/01/a-new-software-that-keeps-politicians-as-honest-as-possible/, retrieved 15 September 2010

TI (2004) *Tools to support transparency in local government*. Urban Governance Toolkit Series. United Nations Human Settlements Programme. March 2004. HS/702/04E.

Available online at: http://www.unhabitat.org/pmss/listItemDetails.aspx?publicationID=1126, retrieved 9 March, 2010.

TI (2010) 'Anti-corruption education and corruption in the education sector'. Available online at: http://www.transparency.org/global_priorities/education, retrieved April 5, 2010

Thomas, C. (2010) 'Why automated sentiment analysis shouldn't feature in social media analysis tools'. 12 March 2010.
Available online at: http://whollysocial.com/index.php/2010/03/why-automated-sentiment-analysis-shouldnt-feature-in-social-media-monitoring-tools/, retrieved 15 September 2010

UNESCO (2007) UN Anti-Corruption Tool Kit 2nd Edition.
Available online at: http://opentraining.unesco-ci.org/cgi-bin/page.cgi?g=Detailed%2F2073.html;d=1, retrieved 14 April 2010, retrieved 15 September 2010

UN (2008) *A Users' Guide To Measuring Corruption*. United Nations Development Programme, UNDP Oslo Governance Centre, Oslo, Norway.
Available online at: http://www.undp.org/oslocentre, retrieved 15 September 2010.

UNDP (2004) *Anti-Corruption. Practice Note*.
Available online at: http://www.sasanet.org/curriculum_final/downlaods/PM/Bibliography/01%20Anti%20Corruption%20-%20Practice%20Note%20UNDP%20-%20WP.pdf, retrieved 15 September 2010

UN (2010) *United Nations Global Compact. Principle 10.* http://www.unglobalcompact.org/aboutthegc/thetenprinciples/principle10.html. Retrieved August 5, 2010, retrieved 15 September 2010

West, D., (2006) 'Global E-Government, 2006'.
Available online at: http://www.insidepolitics.org/egovt06int.pdf, retrieved 15 September 2010

World Bank (2007) *Business Fighting Corruption*. A Business Resource Center. Available online at: http://info.worldbank.org/etools/antic/, retrieved 6 April 2010.

World Bank (2010a) *Introduction to e-Government*. The World Bank e-Government Practice Group. http://web.worldbank.org/wbsite/external/topics/extinformationandcommunicationandtechnologies/extegovernment/0,,contentmdk:20694335~pagepk:210058~pipk:210062~thesitepk:702586~iscurl:y,00.html, retrieved 31March 2010.

World Bank (2010b) *Policies and Institutions for Environmental Sustainability*. http://web.worldbank.org/wbsite/external/topics/environment/extdatasta/0,,contentmdk:21115900~menupk:2935553~pagepk:64168445~pipk:64168309~thesitepk:2875751,00.html, retrieved 31 March 2010.

Information and Communication Technology for Transparency in Sub-Saharan Africa

Rebekah Heacock & David Sasaki

With the exception of Botswana, Mauritius and Cape Verde, none of the countries in sub-Saharan Africa fall above the midway point of the 2009 Transparency International (TI) Corruption Perceptions Index, which measures how citizens perceive the level of government corruption (Transparency International, 2009a). In its profile on the region, TI writes that corruption risks 'undermining political stability as well as the governments' capacity to provide effective basic services.... In such a context, corruption levels can mean the difference between life and death' (Transparency International, 2009b). A number of studies and anecdotes show how increased transparency leads to increased performance and responsiveness in government and the private sector. Transparency initiatives have led to a 20 percent reduction in the number of people hospitalized for food-related illnesses (Linden, 2010), the design of safer cars (Fung, Graham and David Weil,

2007) greater flows of foreign direct investment (Drabek and Payne, 2009), and more efficient financial markets (Austin and Gravelle, 2007). In a cross-national study Michelle S. Mahoney and Paul Webley have found a positive relationship between transparency and trust in government (Mahoney and Webley, 2004). Other studies highlight adverse effects of poorly designed transparency initiatives (Fung, Graham and Weil, 2007; Mattozzi and Merlo, 2007).

While there are undeniably multiple challenges in sub -Saharan Africa concerning technology for transparency projects, such as poor Internet infrastructure (Kaonga, 2008) technophobia, high connection and connectivity costs, the lack of information and communication technology (ICT) policy in some countries and inadequate knowledge and ICT personnel, there is a growing number of government and non-government initiatives.

Ghana's Ministry of Information recently announced the 'Ghana Policy Fair 2010', a showcase of government projects and policies open to public comment (Annan, 2010). In Cape Verde, the Núclea Operacional da Sociedade de Informação, or Operational Nucleus of the Information Society, makes information on the government's financial activities accessible to citizens while allowing them to apply for a variety of civil services – birth and marriage certificates (Núclea Operacional da Sociedade de Informação, 2010). The Portal do Governo da República de Angola offers a similar service in Angola (Governo da República de Angola, 2010).

Civil society has also begun to move its transparency and accountability efforts online. These efforts are supported by a growing technological community in sub-Saharan Africa. Ushahidi, the crowd-sourced reporting tool first developed to track post-election violence in Kenya in 2007 has become known worldwide (Ushahidi, 2010). Ushahidi has sparked a wave of election monitoring projects that utilize the tool, both in Africa and in other regions. The crowd-sourced reporting tool has also been deployed in Togo, and a project is being

planned in time for the 2011 elections in Liberia. In addition to election-related projects, Ushahidi has also been deployed to track medical supply shortages in eastern Africa, xenophobic attacks in South Africa, and conflict in the eastern Democratic Republic of the Congo.

A GROWING COMMUNITY OF TECHNOLOGY-SAVVY AFRICANS

Though Africa's technological community is growing, lack of access to ICT is still a major obstacle to the use of technology for government accountability projects. In all but a few African countries, less than ten percent of the population has Internet access (Internet World Stats, 2010). Mobile phones – some with data services, but most with only simple texting abilities – have fared much better, with penetration rates reaching around 30 percent continent-wide (Smith, 2009). Nevertheless, despite low rates of Internet and mobile phone penetration compared to the rest of the world, sub-Saharan Africa is home to a vibrant community of ICT entrepreneurs, web companies and software developers who are responsible for mobile social networking applications, local blog aggregators and much more. Technology incubators like, Appfrica Labs (Appfrica, 2010) in Kampala and iHub (iHub, 2010) in Nairobi, are fostering new developments in this space.

Parallel to the growing number of technology-savvy young entrepreneurs and activists, there is however a lack of government capacity to use ICT effectively to improve public services delivery and increase transparency. This capacity gap is one of the factors that prompted the founders of the Kenyan Budget Tracking Tool to work with various ministries to put budgetary data online in a way that would be useful for citizens (Heacock, 2010a). Philip Thigo, one of the project's co-founders, says that the government was more or less willing to make its data accessible – and in fact was attempting to put information online (Constituencies Development Fund, 2010) – but that the ministries lacked the necessary technical skills

to make their databases easily navigable by average Kenyans.

Case: Budget Tracking Tool
Despite extensive development assistance, the number of Kenyans who are classified as poor grew from 29 percent in the 1970s to almost 60 percent in 2000. Philip Thigo, who co-heads the Budget Tracking Tool, finds this unacceptable. 'Democratic governance is important, but economic governance is really at the centre of it,' he believes. This conviction led Thigo and partner John Kipchumbah to create a system that enables Kenyan citizens to examine the national development budget in detail, holding their elected officials accountable for the development projects they have promised.

The Budget Tracking Tool focuses specifically on the Constituencies Development Fund, through which Kenyan Members of Parliament allocate money for various projects. Thigo explains, 'that amount of money is supposed to be spent in a democratic manner, meaning that the constituents or the communities have to be consulted'. The Budget Tracking Tool provides information on how much money has been allocated and for which projects, allowing Kenyans to see whether Members of Parliament are following through on their promises.

In addition to building a searchable website, the Budget Tracking Tool also developed a script to handle simple queries via text message, so that anyone with a mobile phone can text in and find out how much money has been allocated for various projects in their area. The system currently gets between 4000 and 4500 queries per month.

In Uganda, Women of Uganda Network (WOUGNET) has held the Ugandan government accountable to women, successfully working to insert gender-sensitive language into the country's national ICT and development policies. And during the presidential elections, Sudan Vote Monitor received hundreds of reports, despite having the site blocked in the country for several days. One of the most important elements of the success of these projects is the involvement of the communities in which they operate. Another key aspect of many of these projects is their willingness to incorporate multiple forms of communication, using the Internet and mobile phones where possible but also extending their outreach to community meetings, radio and printed materials when necessary. WOUGNET for example circulates a print version of its e-mail newsletter for women who are not able to get online.

Case: Mzalendo
Mzalendo means 'patriot' in Swahili. The project began at the end of 2005 with the mission to 'keep an eye on the Kenyan Parliament'. Co-founder Ory Okolloh explains that the idea for the project came about after the website for Kenya's Parliament was shut down following protests by some MPs who were embarrassed about their CVs being published online.

'Beyond providing some level of scrutiny of Kenyan MPs,' Ory writes, 'we built Mzalendo to demonstrate that there is only so much bemoaning you can do about your representation'. Rather, Mzalendo hopes to convince Kenyans – especially young, technology-savvy Kenyans – to engage with their MPs and current legislation. Unlike the profile pages of the official parliamentary website, Mzalendo allows users to leave comments on the profile page of each MP. There was a sense of optimism around Mzalendo's ability to provide voters with pertinent information about their MPs in the run-up to the 2007 Kenyan general election. Several political aspirants made themselves available for interviews and discussions on the website and some online discussions, which took place on the constituency profile pages, turned into offline meetings focused on better policy and governance. That optimism, however, quickly turned into frustration when the contested presidential election between Mwai Kibaki and Raila Odinga led to violence throughout much of the country. An estimated 800 – 1,500 Kenyans were killed and around 200,000 were displaced from their homes. It also led to a period of reduced activity on the website.

Now, with a small amount of seed funding from Omidyar Network, they are preparing to rebuild the website, enable mobile participation, and hire content producers to follow up on investigative stories related to corruption and the performance of MPs. The ambition is now that by the 2012 general election Mzalendo will have enough content to produce voter cheat sheets which rank incumbents by their participation and performance in parliament.

http://transparency.globalvoicesonline.org/project/mzalendo

RESISTANCE TO TECHNOLOGY FOR TRANSPARENCY AND ANTI-CORRUPTION PROJECTS

Governments do not publish information about their activities and budgets for a number of reasons, including lack of resources, lack of technical expertise, and the fear of inviting criticism and exposing corrupt behaviour. In some countries, access is threatened by governments wary of citizens using new communication tools. According to an OpenNet Initiative report on Internet filtering in the region, while many governments are actively attempting to increase ICT penetration, some are blocking online content or monitoring citizens'

Internet use (OpenNet Initiative, 2009). The Sudanese government recently blocked the election monitoring site Sudan Vote Monitor and YouTube during the country's presidential elections (Sudan Tribune, 2010). In a number of countries, including Ghana, Ethiopia, Nigeria and Zimbabwe, Internet service providers and Internet cafés are required to hand over data on customers' online activities to the government if asked. This kind of government intervention may discourage those who might otherwise engage in transparency efforts online.

Resistance may also come from citizens who do not see value in new technologies. Goretti Amuriat, the ICT Program Manager for WOUGNET, says that when the organization was initially surveying women to see how best to develop ICT initiatives, many women in rural communities were uninterested in using technology, preferring to focus their time and energy on more widely available and accessible tools. Earlier this year, reports on an e-governance program in Southern Sudan revealed that a lack of enthusiasm for technology on the part of government officials led to the program's failure (Heacock, 2010b).

The efforts to increase transparency and curb corruption by using ICT in sub-Saharan Africa are currently driven by a few strong visionaries, most of whom have outside support. While they have been able to encourage greater government accountability in some cases, their projects are still often underutilized. A large part of this lack of adoption is the technical difficulties noted above, but in many African countries transparency activists must work hard to convince citizens that pushing for government accountability is more important than other development issues. Mikel Maron from Kibera, Kenya, says: 'It's very much a day to day place, people are concerned with getting dinner tonight, and when you're working on a project which requires a long term individual commitment without immediate rewards, well that's understandably counter to the usual way of thinking' (Heacock, 2010c). As both technology and economic development spread in Africa,

this may change, but for now, it is still something transparency activists must take into account when planning interventions.

AID TRANSPARENCY NEXT IN LINE

A policy briefing entitled 'Greater aid transparency: crucial for aid effectiveness', Sam Moon and Tim Williamson show how a lack of aid transparency can reduce the ability of taxpayers to hold their governments accountable because it is unclear which projects are government-funded and which are donor-funded (Moon and Williamson, 2010). A lack of aid transparency also leads to a lack of government budget transparency, the authors argue. 'Without transparency, discrepancies between aid received and aid spent is hard to measure, and corruption is harder to track and eliminate'.

A substantial amount of donor money pours into sub-Saharan Africa each year – approximately $50 billion, in fact – but the effects are difficult to discern, and a growing number of academics and activists are calling for a halt to the flow (Moyo, 2009). Zambian economist Dambisa Moyo has called foreign aid 'an unmitigated political, economic and humanitarian disaster', and Ugandan journalist Andrew Mwenda delivered a talk at TEDGlobal 2007 in which he argued that aid is preventing Africa from developing (Mwenda, 2007). Several aid transparency initiatives are using technology to open up aid flow data to the public, including the International Aid Transparency Initiative, Aid Info, and the Ujima Project, which focuses specifically on Africa (Ujima, 2010). These initiatives are based on a moral argument that funders aiming to promote more accountability through transparency should also encourage greater accountability of their own work by publishing more information about their spending and activities.

There is room for greater partnership between these types of initiatives and country-specific projects like Kenya's Budget Tracking Tool that would help track aid flows from the inter-

national level all the way down to local project implementation.

Moreover, there is a growing consensus around the need to work towards greater aid transparency. The challenge and disagreement now lie in how. For example, what is the ideal level of granularity for financial information regarding grants? Does publishing the salaries of individual employees violate their privacy? How timely should information be made available? In what format should it be published? How is information across various funders easily accessed, aggregated, and understood? What are the most efficient processes to integrate the publication of information with accounting from the funder's side and budgeting from the recipient country's side? Should future budget information be made available in addition to past investments and current spending?

These are difficult questions and their difficulty probably lies more in how each institution manages their record keeping than ideological differences related to privacy and power. Fortunately, a number of new initiatives are underway to help develop standards around aid transparency. Foremost among them is the International Aid Transparency Initiative, a 'temporary coalition of donor governments, governments of developing countries and NGOs' [non-governmental organizations] that was formed at the 2008 Accra Agenda for Action, which grew out of the 2005 Paris Declaration on Aid Effectiveness. According to its website, International Aid Transparency Initiative's role is to develop consistent and coherent international standards for the way donors report information about aid spending' (Aid Transparency, 2010).

Case: Ujima Project
The Ujima Project is a collection of databases, documents and other information that attempts to bring transparency to the workings and spending of African governments, multinational non-governmental organizations and business enterprises in African countries. Because few African countries have freedom of information laws, getting at this information from inside the countries can be difficult.

The Ujima Project can be described as 'reverse transparency'. Although the information might be hard to come by in African countries, aid donors, international organizations and agencies maintain a wealth of data pertaining to the continent. While this information is public, it tends to be scattered among governments in the United States and Europe, and international organizations like the Global Fund. The Ujima Project takes the information from the various sources and puts it into one easily searchable place.

Parallel to the open database, mass media is regarded as a crucial component in making aid flows more visible to the public. The Ujima Project Website actively supports the work of African journalists and editors by offering African media-professionals easy access to aid-related information. The Ujima Project is a project of the Great Lakes Media Institute, initially founded to support the training of Rwandan journalists and the resulting Great Lakes Media Center in Kigali. Investigative Reporters and Editors, an international journalism organization of investigative reporters and editors based at the University of Missouri-Columbia, has played a key role in the development and support of this endeavour.

To visualize aid flows, weapon sales, and lobbying expenses at the country level throughout Africa, the Ujima Project takes data from USAspending.gov, the United States Department of Justice, the US Department of State, the Global Fund to fight HIV/AIDS, tuberculosis, and malaria, and the UK's Department for International Development. It is managed by the Great Lakes Media Institute in Rwanda and the website was developed by Appfrica, a Uganda-based web development firm.

THE ROLE OF TECHNOLOGY IN AID TRANSPARENCY

Efforts to increase transparency are heavily dependent on making data accessible in the true sense. Some innovative projects have already been developed to help visualize development assistance.

Besides Ujima (Consult case box), Aidinfo.org is a project that researches the current supply of and demand for information related to aid. A recent blog post admits that several of the team's assumptions at the outset of the project have been

challenged during their subsequent research, 'most notably the idea that if more aid information is made available, people will use it'. They have also found that 'donors publish a lot more information than some of us thought, it's just not in a format that's useful for most users. In particular it's often not timely or comparable'. Most importantly, they stress that information related to 'aid and other resources flowing from donor countries' needs to be linked to 'the wider accountability movement in recipient countries where most stakeholders are interested in transparency of the whole budget'. That doesn't make aid transparency less important, only more complicated. The momentum of the aid transparency movement is palpable, but increasing the amount of available data without greater coordination and aggregation, will lead to more confusion than clarity. Raw data must be presented in ways that are easy to understand, and easy to directly tie into at local and national level in each country. Moreover, ambitious international transparency initiatives need to form partnerships with local and national accountability initiatives in order to realize the true potential of these efforts to increase transparency within the sector of development assistance and elsewhere.

For more information please consult:

Technology for Transparency – The role of technology and citizen media in promoting transparency, accountability and civic participation.
Editor: David Sasaki.
www.transparency.globalvoicesonline.org

REFERENCES

Aid Transparency (2010) 'About Aid Transparency', http://www.aidtransparency.net/about.

Annan, L. (2010) 'Is Ghana's First-ever Policy Fair a Smart Move?', *Global Voices Online*, April 30, 2010,http://globalvoicesonline.org/2010/04/30/is-ghana's-first-ever-policy-fair-a-smart-move/.

Austin, D. A. and Gravelle, J., G. (2007) 'Does Price Transparency Improve Market Efficiency? Implications of Empirical Evidence in Other Markets for the Health Sector', *CRS Report for Congress*, http://www.fas.org/sgp/crs/secrecy/RL34101.pdf.

Constituencies Development Fund (2010) 'Board Disbursements', http://www.cdf.go.ke/index.php?option=com_content&task=category&sectionid=32&id=106&Itemid=85.

Drabek, Z. and Payne, W. (2009) 'The Impact of Transparency on Foreign Direct Investment', *World Trade Organization Economic Research and Analysis Division*, http://ideas.repec.org/p/fth/wtoera/99-02.html.

Fung, A., Graham, M., and Weil, D. (2007) *Full Disclosure: The Perils and Promise of Transparency*. Cambridge: Cambridge University Press

Heacock, R. (2010a) 'Budget Tracking Tool', *Technology for Transparency Network*, http://transparency.globalvoicesonline.org/project/budget-tracking-tool.

Heacock, R (2010b) 'Sudan: Is ICT All it's Cracked Up to Be?' Global Voices Online, March 4, 2010, http://globalvoicesonline.org/2010/03/04/sudan-is-ict-all-its-cracked-up-to-be/

Heacock, R. (2010c) 'Map Kibera', Technology for Transparency Network, http://transparency.globalvoicesonline.org/project/map-kibera.

iHub (2010) http://www.ihub.co.ke/.

Kaonga, V. (2008) '*The Internet as a Journalistic Tool: Analysing the Use of Internet in Malawi's Radio Stations*', Örebro University, http://www.magj.se/pdf/Vic-

tor%20Kaonga.pdf.
Linden, R. (2010) 'Transparency Breeds Self-Correcting Behavior', *Governing*, January 13, 2010, http://www.governing.com/columns/mgmt-insights/Transparency-Breeds-Self-Correcting-Behavior.html.

Mahoney M., S. and Webley, P., (2004) "The Impact of Transparency: A Cross-National Study," University of Exeter, http://www.fig.net/news/news_2004/mahoney_webley.pdf.

Mattozzi, A. and Merlo, A. (2007) 'The Transparency of Politics and the Quality of Politicians', *Penn Institute for Economic Research*, January 2007, http://economics.sas.upenn.edu/system/files/07-008.pdf.

Moon, S and Williamson, T (2010) 'Greater Aid Transparency: Crucial for Aid Effectiveness', *Overseas Development Institute*, Project briefing no 35, http://www.odi.org.uk/resources/download/4673.pdf.

Moyo, D (2009) 'Why Foreign Aid is Hurting Africa', *The Wall Street Journal,* March 21, 2009, http://online.wsj.com/article/SB123758895999200083.html.

Mwenda, A (2007) 'Andrew Mwenda Takes a New Look at Africa', TED.com, June 2007, http://www.ted.com/talks/andrew_mwenda_takes_a_new_look_at_africa.html.

OpenNet Initiative (2009) 'Internet Filtering in Sub-Saharan Africa', *OpenNet Initiative*, http://opennet.net/sites/opennet.net/files/ONI_SSAfrica_2009.pdf

Sudan Tribune (2010) 'Sudan Reportedly Blocks YouTube over Electoral Fraud Video', April 22, 2010, http://www.sudantribune.com/spip.php?article34836.

Transparency International (2009a) 'Corruptions Perception Index', http://transparency.org/policy_research/surveys_indices/cpi/2009/cpi_2009_table.

Transparency International (2009b) 'Corruption Perceptions Index 2009 Regional Highlights: Sub-Saharan Africa', http://transparency.org/content/download/47603/761859/CPI+2009+Regional+Highlights+Sub-Saharan+Africa+_en.pdf.

Ujima Project (2010) 'The Ujima Project' http://ujima-project.org/

Mobile Technology as a means to fight corruption in East Africa

Johan Hellström

This paper explores the role of mobile technology as a means to promote good governance, increase accountability and fight corruption. It will give a general overview of governance in relation to mobile services looking into the specifics of mobile technology as a way to fight corruption. For a better understanding of both the potential and challenges in using mobile technology, it will analyse relevant cases with a focus on Uganda. The study draws from data generated through desk research and in-depth interviews, meetings and discussions with key stakeholders in East Africa.

BACKGROUND

Corruption constitutes a serious obstacle for many developing countries. Definitions vary but the standard definition of

corruption is the abuse/misuse of public office for private gain (Svensson, 2005; World Bank, 2010) where government officials 'charge personally for goods that the state officially owns' (Shleifer and Vishny, 1993:599).

Corruption seen as bribes has several similarities to taxes but differs in some crucial ways – the obvious one being that tax goes into the treasury while bribes goes into the pocket, but also that 'unlike taxation, corruption is usually illegal and must be kept secret' (Shleifer and Vishny, 1993: 612).

Corruption does not necessarily involve monetary exchange. Inefficiency or when public servants fail to deliver services that have been paid for by the government could be seen as a form of 'quiet corruption'. The World Bank states in the report 'Africa Development Indicators 2010' that quiet corruption indicate 'various types of malpractice of frontline providers (teachers, doctors, inspectors, and other government representatives)' (World Bank, 2010: xi) and that these behaviours 'include both potentially observable deviations, such as absenteeism, but also hard-to-observe deviations from expected conduct, such as a lower level of effort than expected or the deliberate bending of rules for personal advantage' (World Bank, 2010: xi).

No matter how corruption is defined, it weakens societies and impacts and hinders social and economic development. It diverts domestic and foreign investment away from where it is needed; it weakens education and health systems; exacerbates inequality; distorts electoral processes and undermines government institutions (United Nations Development Programme and United Nations Office on Drugs and Crime, 2009)

Measuring corruption is difficult 'due to the secretive nature of corruption and the variety of forms it takes' (Svensson, 2005:21). Nevertheless, there are at least three different measures of corruption available (Svensson, 2005):

1. Data from private risk-assessment firms. Popular among global companies is the corruption indicator produced by Political Risk Services (PRS) (www.prsgroup.com/) and published in the International Country Risk Guide. The corruption indicator tries to determine the political risk involved in corruption.
2. Data from perception-based sources. An example is the Corruption Perceptions Index (CPI) constructed by Transparency International (TI) (www.transparency.org/), which is widely used among policymakers. The indicator tries to determine a country's level of corruption based on the overall extent of corruption and indicates the perceived level of public-sector corruption in the country.
3. The Worldwide Governance Indicators project is constructed by the World Bank and reports aggregate and individual governance indicators for six dimensions of governance where Control of Corruption is one. The Worldwide Governance Indicators has a broader definition of corruption and tries to measure the extent to which public power is exercised for private gain, including petty and grand forms of corruption, as well as 'capture' the state using a wide range of sources.

CORRUPTION TRENDS IN EASTERN AFRICA

According to Svensson (2005) there is a strong correlation between the different measures on the ranking of a specific country even though definitions and aggregation methods might differ. Using the three measures for comparison, the East African countries support this conclusion (Table 1).

According to all three corruption measures, Kenya is the most corrupt country in East Africa, followed by Uganda and Tanzania. Rwanda is the least corrupt in the region. Small improvements can be seen in 2009 compared to 2008 in all countries except Tanzania who, according to both TI and the World Bank, seems to go in the wrong direction. However, PRS ranks Tanzania higher in 2009.

Table 1. Three measures of corruption, East Africa

Country	International Country Risk Guide			Corruption Perceptions Index			Control of Corruption*		
	Rank 2008 (Aug, 140 countries)	Rank 2009 (July, 140 countries)	Corruption Comp. 2009 (July, Max. = 6)	Rank 2008 (180 countries)	Rank 2009 (190 countries)	CPI Score 2009 (Max = 10)	Rank 2007 (100% = highest ranking)	Rank 2008 %	Corruption Indicator 2008 (low -2.5 to high 2.5)
Kenya	117	111	1.0	147	146	2.2	14	14	-1.01
Rwanda	N/A	N/A	N/A	102	89	3.3	58	59	0.03
Tanzania	100	87	3.0	102	126	2.6	41	36	-0.51
Uganda	115	109	2.0	126	130	2.5	23	23	-0.79

Source: PRS Group 2010a, PRS Group 2010b, TI 2010, World Bank 2009. *2009 N/A

Looking at TI's CPI data from 1999, the perceived level of public-sector corruption in East Africa during the past decade has gone down (See Table 2).

Table 2. Corruption Perceptions Index 1999 and 2009

Country	Corruption Perceptions Index		
	Rank 1999 (99 countries)	CPI Score 1999 (Max = 10)	CPI Score 2009 (Max = 10)
Kenya	90	2.0	2.2
Rwanda	N/A	N/A	3.3
Tanzania	93	1.9	2.6
Uganda	87	2.2	2.5

Source: TI 2010

MOBILE TECHNOLOGY TRENDS IN EASTERN AFRICA

The positive development in terms of reduced corruption could be the result of government interventions, higher salaries to public officials and donor strategies. However, an alternative explanation could be that the very presence of a decentralised information and communication network produces demands for better public services. This hypothesis is supported by research conducted by Bailard (2009) who draws CPI and mobile data from 46 nations over the period 1999 (before mobile phones were widely used) to 2006 (when mobile phones were widely used) and concludes that 'a fixed

effects regression of panel data reveals a significant negative correlation between a country's degree of mobile phone penetration and its level of perceived corruption' (Bailard, 2009: 341). Why does a higher mobile phone penetration lead to lower levels of perceived corruption? Bailard argues that:

the net effect of the rapid and massive diffusion of mobile phones in Africa will be the reduction of corruption by decentralizing information and communication, thereby shrinking the veil of secrecy that shields corrupt behavior as well as altering the cost-benefit calculus of corrupt behavior by strengthening oversight and punishment mechanisms (Bailard, 2009: 350).

Could this also be the case for East African countries? Indeed, the level of perceived corruption has gone down according to CPI and the mobile phone penetration has exploded (see Table 3). Thanks to technological advancements, lower handset prices and the deregulation and privatisation of the telecommunications industry, mobile technology has become more affordable. As a result, there are 50 million mobile subscribers in the region and people spend almost 50% of their disposable income on mobile communication.

Table 3 shows the penetration rate (percentage of people with an active SIM card i.e. number) in 2003 and at the end of 2009, the penetration rate, the total number of subscribers, percentage of the population covered with a mobile signal,

Table 3. Mobile statistics, East Africa

Country	Penetration rate, Q4 2003	Penetration rate, Q4 2009	Subscribers, Q4 2009 (Millions)	Mobile coverage (population)	Mobile expenditure of disposable income, 2007-08	Operators
Kenya	5%	46%	18,5	84%	53%	4
Rwanda	2%	20%	2 0	~100%	66%	3
Tanzania	2%	43%	17.5	N/A	29%	6
Uganda	3%	36%	11.8	~100%	49%	7

Source: Industry data, ITU 2009, ITU 2010, Communications Commission of Kenya (CCK) 2009, Tanzania Communications Regulatory Authority (TCRA) 2010, Chabossou et al. 2009

monthly mobile expenditure as a percentage of monthly disposable income, and the number of mobile operators in each of the four countries.

Nevertheless, despite the small improvements during the past decade, corruption remains pervasive throughout the region. Reinikka and Svensson (2006) in their article 'The Returns from Reducing Corruption: Evidence from Education in Uganda'state;

However, one conclusion we draw from the Uganda experiment is that since traditional approaches to improve governance have produced weak results in most developing countries, experimentation and evaluation of new tools to enhance accountability should be an integral part in the research agenda on improving outcomes of social services.

Intelligently deployed information and communication technology (ICT) solutions could constitute new tools as they can play a vital role in improving transparency, accountability and participation. However, for various reasons, available tools have hardly been used in a strategic manner and the rather few existing cases are often labelled success stories despite the lack of recipes for sustainability and/or scaling-up. Nevertheless, the extraordinary growth in the use and availability of mobile devices and services in recent years might open up new possibilities.

THE POTENTIAL IN MOBILE SOLUTIONS

Access to mobile telecommunications and the innovative use of mobile phones are often described as the universal panacea. There are a number of promising initiatives looking at citizen-to-government accountability using mobile solutions in East Africa. The organisation Twaweza based in Tanzania attempts tracking teacher and pupil attendance and absenteeism in Ugandan primary schools and the Budget Tracking Tool in Kenya helps citizens to monitor and track both disbursements

and utilisation of developments funds (see Table 4 for more information). However, looking at the developments in the health, agriculture and finance sectors, where many mobile applications have been rolled-out and scaled-up, mobile interventions to improve transparency, accountability and participation are still struggling.

Looking at the potential in using mobile solutions for good governance purposes, the possibilities are endless. Access to mobile phones empowers the individual in many ways as it opens up a two-way dialogue – interaction with both government and other citizens. Mobile phones make everyday communication more efficient and increase efficiency in daily activities as they help in time management and general organisation.

Mainly it is the interplay of four elements that creates a virtuous circle of innovation that can benefit all citizens (McNamara in Hellström, 2010):

- Access – innovations in network design, communications hardware and infrastructure financing are steadily expanding the mobile 'footprint' to cover a larger percentage of the population;
- Affordability – relatively low total cost of ownership, due to the combination of prepaid service plans and cheaper mobile handsets, makes it easier for citizens to afford and use mobile services;
- Appliance innovation – the growing multi-functionality of mobile devices and innovations are making these devices more adaptable to a range of needs and services relevant to all citizens;
- Applications – there has been a vast increase in the past few years in the development and roll-out of mobile applications.

Under the best circumstances, these virtuous circles will ultimately lead to increased participation where citizens will demand improved, more transparent, accountable and re-

sponsive governance where they see public services as their right. According to McNamara, mobile devices and services can help citizens 'connect with one another for more effective collective action [...] in demanding improved, more transparent and responsive governance and public services' (Hellström, 2010: 41).

A growing body of evidence

There are a number of anecdotal stories from around the world where the mobile phone is used in anti-corruption. For example, the Zimbabwe corruption case where the defendant was recorded soliciting a bribe; the witness simply waited for the right opportunity and then recorded the entire conversation using his phone (Textually, 2006). In 2008 in India the Central Bureau of Investigation launched a campaign urging India's citizens to report, via Short Message Service (SMS), government corruption. The basic idea of the campaign is to build a database of officials who need to be watched (Rajaratnam, 2008). In Pakistan, civil servants working with land transfers must, via SMS, submit transactions data stating the amount paid and the mobile numbers of the buyer and seller. The senior officials can then make spot checks on these transactions (The Economist, 2009). Similar systems could be applied in situations where rural citizens receive government funding via local government.

Also in East Africa, the mobile phone has been used to improve service delivery, transparency, accountability and participation. One-to-many communication though the use of bulk SMS have been used by governments to broadcast urgent news, to send reminders to voters, and to urge citizens to cool down during civil unrest. Various whistle-blowing mechanisms and anti-corruption hotlines have been set up by both civil society organisations and government institutions (e.g. the civil society organisation Anti-Corruption Coalition of Uganda (ACCU) and the public body Kenya Anti-Corruption Commission, (KACC). There is also a growing number of examples where mobile phones have been used as a citizen-based monitoring and crowd-sourcing tool during disasters,

crises and elections (see Ushahidi and Ugandawatch 2011 below in Table 4 and the Violence-Prevention-Tool initiated by Oxfam in Kenya) and as a data collection tool during census count and parallel vote tabulation (e.g. OpenXData, www.openxdata.org, RapidSMS, www.rapidsms.org, FrontlineSMS, www.frontlinesms.com/).

Call-in radio shows are very popular all over East Africa. Daily shows and weekly programmes discussing politics are other examples of how mobile phones can make politics and governments more transparent. Jussi Impio from Nokia Research Africa, says 'people have phones, and when politics is being discussed they can call anonymously and say things journalists cannot discuss […] Newspapers have started to quote them, and journalists say it has given them more freedom to discuss corruption' (The Economist, 2009:5). In Burundi, the World Bank Institute, in partnership with International Alert and Burundi's Radio Publique Africaine, run a call-in radio program targeting the youth. The idea is to disseminate third-party studies on corruption and poor governance and let audiences be part of the following discussion by providing a safe space for young people to be heard (World Bank Institute, 2010)

Table 4 list some of the more direct applications implemented in East Africa, addressing various forms of corruption.

Table 4. Mobile applications addressing accountability, transparency and participation

Country	Project	Description
Citizen-to-government interaction	2888 (Kenya)	An SMS service that allows Kenyans to send information, suggestions, complaints etc. via SMS to number 2888, the Office of Public Communications. The aim is to increase citizen-to-government communication and sensitize the government spokesperson to the priorities of Kenyans. The service will also help in tracking and apprehending corrupt officials. The service was highly promoted during the food crises in 2009 as a way to ease communication. It was launched in June 2005. www.communication.go.ke/
	e-Service Delivery Project (Kenya)	Information on progress of identity card (text 2031) and status of passport (text 2032). The government and Kenya's ICT Board will expand this service to cover other key areas of service delivery such as land and health and are working with a company which is digitizing content for varies ministries of the government. The e-Service Delivery Project is run by the Ministry of Migration and Directorate of e-Gov. www.e-government.go.ke/

Country	Project	Description
Disaster and crises management	Ushahidi (multiple countries)	The Ushahidi platform developed in Kenya is used all over the world for different cases of good governance related intervention. The crowd-sourcing tool was originally developed and used for post-election monitoring in Kenya 2007/8. Ordinary citizens can report incidents using multiple channels such as the web, emails, SMS and Twitter. Cases are then verified and mapped. Ushahidi is a good example of crowd-sourcing and how mobile phones provide a good complement to government lead governance by adding the dimension of quick participation and action regarding certain issues. So far the platform has been used mainly during emergencies like natural disasters and man-made crises but also for election monitoring and citizen participation. It islike BungeSMS mentioned below and Mi Panamá Transparente in Panama. The latter project (implemented by the Panaman chapter of Transparency International and the International Centre for Journalism amongst others) provides the opportunity to complain about crime in general and corruption cases in particular (see www.mipanamatransparente.com). www.ushahidi.com/
Monitoring attendance and absenteeism	CU@SCHOOL (Uganda)	Recent research indicates that primary school teachers in a number of African countries are absent from school 15–25 percent of the time and that many of those in school are not found teaching, i.e. low effort (World Bank 2010). The organisation Twaweza, in collaborating with SNV Uganda, tries to address this problem. The project facilitates the monitoring of teacher and pupil attendance and absenteeism in primary schools by using an SMS based information system. The project will pilot an SMS application that generates frequent and detailed overviews of teacher and pupil attendance in 100 primary schools, selected in 2 districts. The information will make the dynamics around teacher absenteeism transparent and will inform district and sub-district government officials, well as non-state actors at (sub) district level, so that they take appropriate short, medium and long term action, as. http://twaweza.org/
Mobilisation and citizen-to-government interaction	BungeSMS (Kenya)	Empowers citizens to influence local governance in their constituency through the use of SMS and the Web. It intends to strengthen citizen-to-government (bottom-up) communication in governance. An SMS to a Member of Parliament (MP) is sent to a designated number and routed to the BungeSMS website. On the BungeSMS website, it is mapped onto Google Maps using the Ushahidi platform. Run by Made In Kenya Network. Send SMS to 3454. www.bungesms.com
Accountability	Budget Tracking Tool (Kenya)	The Budget Tracking Tool is a collaborative platform for grass roots communities to actively engage in public resource management. It enables citizens to monitor and track both disbursements and utilisation of development funds: projects funded by Constituencies Development Fund (CDF, www.cdf.go.ke/), Local Authority Transfer Fund (LATF, www.localgovernment.go.ke/), Women's Fund and Youth Fund. The tool can be accessed via the Web and by SMS by sending a text message to 7002, e.g. constituency#project (westlands#water). It can also be used for feedback in the format #constituencyname#projectname#comments. The tool has been developed by the Social Development Network and designed by Infonet. www.sodnet.org www.opengovernance.info
Monitoring election fraud and malpractices	Ugandawatch 2011 (Uganda)	Ugandawatch 2011 is run by Democracy Monitoring Group (DEMGroup, www.demgroup.org), which is a consortium of four civil society organisations that have come together to contribute to freer, fairer, transparent and credible elections in Uganda. The members of DEMGroup are Uganda Joint Christian Council (UJCC), Action for Development (ACFODE), Transparency International Uganda (TIU), and the Centre for Democratic Governance (CDG). UgandaWatch 2011is an independent hotline where citizens can report any problems they face with the electoral process. SMSs are sent to 6090 for the cost of 100UGX. There are 6 channels: 1) Refusal to register, 2) Voter registration is not accessible, 3) Wrong voter registrations, 4) Gender issues, 5) Money and politics, 6) Violence and intimidation. The service is 'Powered by Managing News. Fuelled by Mountbatten. Managed by DEMGroup.' Besides following up these issues with the responsible organisations involved (e.g. EC), they also make reports available on their website. The number to SMS is 6090 and costs 100UGX. Works on all networks. http://www.ugandawatch2011.org/
	Miscellaneous short codes (Kenya, Tanzania, Uganda)	Even though designed for voice they are worth mentioning: regional numbers are 112 for emergency/police/SOS, 114 for fire and 115 for ambulance. In Kenya and Tanzania there are some designated short codes for 'Crime Stoppers' (111) and 'Anti-corruption' (113). In Tanzania, if you call 113 you will reach the Prevention of Corruption Bureau. In Uganda, one can leave anonymous complaints on a special hotline (347387) to the Inspector General of the Government (IGG) 'for rapid response to complaints' (IGG, 2009). Kenya Anti-Corruption Commission (KACC) has a similar system in place.

Source: TI 2010

Corruption hotlines

Corruption hotlines for voice and/or SMS are usually designed to facilitate the making of complaints. According to Transparency International Uganda (2007) it is important that:

- the role of the organisation/institution providing the hotline and precisely whom the intended beneficiaries are is carefully designed;
- the lines are introduced as part of a larger strategy;
- there is a well-focused advertising campaign explaining the purpose of the service and who is operating it;
- there are clear guidelines on whether and when anonymous information can be accepted;
- feedback is given to the callers (if identified) by reporting back what has happened regarding reported case.

In Uganda, the ACCU has a hotline where citizens can report corruption and other malpractices. Calling the number 0414 662000 will let you speak with the receptionist who will then handle the case accordingly. So far, ACCU have not developed a systematic way on how to follow up on calls: there is no database in place, calls are not mapped and data is not collected and stored. The former coordinator of ACCU, Jaspe Tumuhibise, estimates that roughly 300 calls are made per quarter giving about three calls per day. More people would probably call if the hotline was a toll free service. Setting up a toll free line would cost ACCU almost 300 US$ per month – a very high price for a rather small non-governmental organisation. On top of this they would also have to negotiate the interconnection charges between different operators.

As a way to solve the problems of high costs, they have instead introduced an informal 'beeping system', or call back service, where people beep/flash the hotline number and hang up with the hope that the receptionist to call back. This 'system' costs roughly 100 US$ per month in airtime depending on the number and duration of the calls. ACCU have been in contact with operators to negotiate a complementary toll free service

as part of the service providers' social responsibility programmes but without success up to now. Tumuhibise believes that if the hotline was a free service for the end-user and if it was more automatic, more people would call in. Tumuhibise says that people fear the human interface, as Uganda is a small country and that there is no trust in the system. These factors hinder usage.

Information campaigns

Mobile applications and programmes designed to reach the majority of mobile subscribers, tend to rely on simple, ubiquitous formats like SMS and usually works on any low-end phone. These applications, however, require access to the target population's phone numbers. Mobile operators are usually not too keen to hand out lists of their subscribers' phone numbers and value added service providers see their databases as a commodity.

Organisations and institutions who want to run a successful outreach/publicity campaign using SMS need to create a subscriber database of active phone numbers. Often it is enough to buy the service from a bulk SMS service provider but the risk is that the messages miss their targets.

Building a good database of numbers can be done in many different ways. Numbers and relevant information can be collected at meetings and workshops and by encouraging people to sign up through emails, the organisation website, social media such as Twitter and Facebook, but also through traditional media such as publications, billboards and broadcast media. The more detailed the database (address, gender, preferred language, age etc.) the more targeted the campaigns can be. The Zimbabwean non-governmental organisation Kubatana write in the practitioner's handbook that it is important to:

> get 'buy-in' from the people to whom you wish to send text messages. Otherwise it is likely that you will be accused of sending out 'spam' (unsolicited messages) and you will irritate your constituency rather than encouraging their support (Kubatana, 2008:2).

This is of extra importance for organisations working in a politically sensitive environment. The risk of being accused of 'invasion of privacy and thus run the risk of incurring investigation, fining or closure' (Kubatana, 2008:2) is otherwise high.

In 2008, ACCU ran a 'Name and Shame' campaign, sending out 20,000 SMSs in bulk to selected users urging them to name and shame people in the society who had done something extraordinary or something not too good (i.e. corrupt). The response rate was terribly low (only 262) due mainly to two reasons: people were not sure who sent out the SMS and secondly, they were not sure whether their response would be kept anonymous or not. The risk of tracking and the uncertainty made the campaign rather unsuccessful.

THE CHALLENGES IN USING MOBILE SOLUTIONS TO INCREASE TRANSPARENCY AND REDUCE CORRUPTION

Despite the high number of pilots and anecdotes pouring out of East Africa, how is it so few initiatives are scaled-up? A systematic way to roll-out efficient and sustainable services seems to be missing.

To develop a mobile application is fairly easy from a technological point of view, despite the fact that the mobile sector is fragmented at many levels; from handsets to networks, and that the majority of existent handsets in East Africa are low-end phones with a small screen size. Sophisticated and smart mobile phones with related applications have a tiny distribution in developing countries compared to simple, low-end handsets. SMS applications therefore dominate at present but mobile broadband solutions have the potential to grow in a virtuous circle too where capacity, in terms of technology and technical know-how, drives content, which drives the demand for bandwidth, data services, handsets etc., which drives capacity and supply. A guess is that East Africa's mobile application future is IP (Internet Protocol) based, not SMS based. The simple reason being that a subscriber can do so

much more with a data enabled phone and send messages at a fraction of the cost of SMS.

However, for now and some years to come, SMS and Unstructured Supplementary Service Data (USSD) are going to dominate the scene. However, there are limitations. The SMS message space is very short (160 characters), which means it is best suited for straightforward notifications, announcements, appeals or alerts. SMS can also be used to raise a specific issue but rather than explaining everything in various SMSs, the message can direct the user where to find out more (an address, a website, listening to a specific radio show or reading a specific newspaper).

There are a number of scholars and practitioners (Verclas, 2010; Conley et al., 2010; Mechael, 2008; Mechael et al., 2010) who have tried to identify the challenges in developing, implementing and sustaining mobile applications for social and economic development. The barriers to growth fall into two broad categories;

1. barriers to demand and use; infrastructure (network, electricity), access to devices, literacy, languages, awareness, trust, privacy, affordability, user-friendly and useful content, etc.
2. barriers to content creation and provision; awareness, ICT expertise, tools, sustainability, finance, scalability, innovative business models, etc.

One of the barriers to mobile phone use, especially in rural areas, is access to reliable electricity. With the majority of East African citizens not connected to the national grid, it makes it difficult and costly for people to charge their phones. Many switch off their phones while charging the battery, or just for the purpose of saving batteries. Therefore, urgent and time sensitive communication like emergency alerts etc. might face problems.

Another barrier is affordability. Affordability is also seen as a possibility compared to other technologies and tools available but the total cost of ownership, i.e. cost of a device, airtime, charging, etc., is still too high for many. Data from ResearchICT Africa's Household e-Access and e-Usage Survey from 2007–2008, shows that in East Africa, people spend more or less half of their disposable income on mobile communications (Chabossou et al., 2009). However, there are arguments that people are saving, cutting down on costs and saving money owning a phone but this does not seem to be applicable for people below the poverty line (Chabossou et al., 2009). The end result is that people are not utilising existing services and that many still rely on public payphones and family or friends to make or receive messages and calls.

Finally, surrounding support systems are lacking. If a subscriber runs into technological problems there is no support. Customer service in East Africa is generally non-existent, the general ICT capacity is low and there is a lack of training and skills development.

Privacy and registration

There are some challenges that are a bit more specific in governance related applications. How can anonymity be secured in situations when anonymous submissions and leaks of sensitive information are communicated? How can privacy be assured when data needs to be verified and when sensitive opinion polls are conducted? Until recently this has not constituted a problem in East Africa. A person can still buy a SIM card at every street corner or in any village, put it in the phone, buy airtime and start communicating. The easy access to SIM cards, i.e. that there is no hurdle for the customer to acquire a phone number (together with prepaid service plans and low denomination airtime vouchers) is usually used as an explanation of the phenomenal growth of mobile penetration. Yet, due to recorded misuse of this liberal market and absence of controls, scams, SMS spam and threats are on the rise. Governments are now pressurising operators to begin registering SIM cards and subscriptions, in order to connect a person to

the SIM, as a way of addressing the identified problems and to track criminal and terrorist activity. Registration might reduce the criminal behaviour but will also lead to increased control and central monitoring. Already, phones are being tapped and individuals are being triangulated, for good and for bad. If users lack trust in the technology and in the mobile ecosystem surrounding it, applications dealing with sensitive information will not be used.

Successful whistle-blowing programs build on citizens' willingness to provide information and give evidence. Not only does a whistle-blower often require protection (from physical, social and/or economic retaliation) from the person/s exposed, but also anonymity while reporting the case. If anonymity (or privacy at least) cannot be assured, no one would use the system. The Internet is designed in such a way that it is fairly easy to hide your identity by using a web proxy for example. Mobile phone networks work differently and privacy is much harder to accomplish due to the fact that the mobile networks 'record a phone's hardware signature and SIM. As governments begin registering SIM cards as a way of tracking criminal and terrorist activity, anonymous publishing or reporting via mobile phones grows far more difficult' (Zuckerman, 2009).

Sustainability

From a developer's and implementer's point of view, turning a good idea into a sustainable product or service is critical. The first challenge is to locate initial funding. Another ingredient for a successful mobile solution is a sound financial and operating model to maintain the service. In a context where most of the subscribers have a fairly low disposable income, where 'the commitment of the government to fight corruption is at most selective' (Centre for Basic Research, 2004), and where civil society organisations are heavily dependent on donor funds, innovative business models and billing plans for service delivery are needed. Someone needs to pay for the service and traffic but who? To develop an innovative business model that will take away the cost for the end-user, clearly save costs

for local government, and not depend on donor funding, is hard and will require more research and is outside the scope of this article.

Even the mobile industry itself constitutes a challenge for mobile governance interventions:

The sector is highly competitive and privatised with profit as the primary focus. If a non-profit service is launched it is usually being implemented as part of corporate social responsibility (CSR) programs in the entertainment, sports, housing, health, education and environment sectors, i.e. sectors with maximum reach out, good for marketing purposes and with few political hurdles. Good governance on the other hand is a public good. How does one attain a balance between the two? Today there are few innovative business plans that bring the two worlds together and therefore social and governance applications end up low on the priority scale of operators. Further, public service is a long term commitment, there are no quick fixes which a pilot can fix (Hellström, 2010:55).

DISCUSSION AND CONCLUSIONS

How can the identified challenges be addressed and what is needed to further support the use and development of relevant services? To avoid the 'forever pilot syndrome' that a majority of ICT for development projects have, it is important to design the intervention with scalability in mind. This is of extra importance in the governance field since pilot projects do not really have an impact. Rather what is needed is a service delivery approach with a sound financial and operating model. Analysing various mobile applications in East Africa a number of success factors have been identified. Many of the factors are general but still too often overlooked:

- do the homework (and avoid re-inventing the wheel)
- let it be driven by the end-user (and look at needs)
- fit into already existing user patterns

- consider open standards/content (and build a user community)
- involve the right stakeholders from the start and use local capacity.

In the implementation phase:

- have a viable business model and/or predictable funding flows
- involve end-users in content creation where applicable
- implement a decentralised solution rather than centralised (cross network instead of working only with one operator when possible)
- educate the end-user
- market properly (to get a critical mass of users)
- take time (let it take time to grow)
- continue documentation throughout the process (both success as well as failure)

When designing mobile applications and services that try to address corruption – applications to monitor absenteeism, report corruption, track budgets etc. – it is of high importance that the bigger context is fully understood. Take a whistle-blower application as an example. It is fairly easy to design it technically (i.e. the same as setting up a call centre). However, in reality where mobile phones could be tapped, where the existent whistle-blower protection bill gives no protection and where there is no systematic way to follow up on calls, scaling-up becomes more complex. Issues like privacy, anonymity and security can not be overlooked.

Generally little interaction between citizens and government may also affect the results and impact of a mobile intervention. In Uganda, there are few linkages between citizens and above the lowest level of local governments. The limited interaction between citizens and state institutions leads to a situation where the sense of ownership and the identification with the government/state is low. The fact that a large share of the East African states' budgets is donor funded is problematic

too; people tend to see government services as a favour rather than their right.

Mobile interventions must therefore be followed by educational advertisement and marketing campaigns explaining how to use the service, i.e. for example, a step by step guide as to how to send SMS, why to use the service and who is running the service.

Looking at the few cases that exist in East Africa, mobile phones seem to help to reduce corruption by making it easier to spread the world about malfeasance, and increasing the potential of detection. Mobile phone services can empower citizens, as they improve access to timely information, can engage citizens in participatory monitoring, and support citizen-government dialogue which could create an interactive communication channel. Mobile solutions give citizens a voice, bigger ears and hopefully, a chance to mobilise and act upon the information.

REFERENCES

Bailard, C. S., 2009. Mobile Phone Diffusion and Corruption in Africa. *Political Communication* 26(3): 333–353

Centre for Basic Research, 2004. *Nature, Impact and Extent of Political Corruption at National and Local Government Level*.

Chabossou, A., Stork, C., Stork, M.and Zahonogo. Z., 2009. Mobile Telephony Access and Usage in Africa. *3rd International Conference on Information and Communication Technologies and Development*, April 17–19, 2009, Carnegie Mellon University in Qatar Education City, Doha, Qatar.

Conley, E, Brown, S. and Scharpey-Schafer, K., 2010. Mobile M&E: Experiences from Pilot to National Scale Implementation. *IST-Africa 2010 Conference Proceedings*, Cunningham, P., and Cunningham, M., (Eds) IIMC International Information Management Corporation, 2010. ISBN: 978-1-905824-15-1

Communications Commission of Kenya (CCK), 2009. *Sector Statistics Report April–June 2008/09*. http://www.cck.go.ke/UserFiles/File/SECTOR%20STATISTICS%20REPORT%204th%20Quarter.pdf

Hellström, J., 2010. The Innovative Use of Mobile Applications in East Africa. *Sida Review* 2010:12. ISBN: 978-91-586-4129-7. http://upgraid.files.wordpress.com/2010/06/sr2010-12_sida_hellstrom.pdf

International Telecommunication Union (ITU), 2009 *Information Society Statistical Profiles 2009 – Africa*. http://www.itu.int/ITU-D/ict/material/ISSP09-AFR_final-en.pdf

International Telecommunication Union (ITU), 2010. *Measuring the Information Society- 2010*. http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf

Kubatana, 2008. *How to Run a Mobile Advocacy Campaign*. www.kubatana.net

Mechael, P., 2008. *In Search of Scalable mHealth Solutions*. www.w3.org/2008/10/MW4D_WS/papers/mechael.pdf

Mechael, P., Batavia, H., Kaonga, N., Searle, S., Kwan, A., Goldberger, A., Fu, L.and Ossman, J., 2010. *Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: Policy White Paper*. Center for Global Health and Economic Development, Earth Institute, Columbia University. http://www.globalproblems-globalsolutions-files.org/pdfs/mHealth_Barriers_White_Paper.pdf

Political Risk Services (PRS) Group, 2010a. Country Risk Ranked by Composite Risk Rating. *International Country Risk Guide*. http://www.prsgroup.com/PDFS/sT3B.xls

Political Risk Services (PRS) Group, 2010b. Political Risk Points by Component. *International Country Risk Guide*. http://www.prsgroup.com/PDFS/sT3B.xls

Rajaratnam, L. 2008. *CBI SMS Campaign for Anti-corruption*, http://www.merinews.com/article/cbi-sms-campaign-for-anti-corruption/139622.shtml

Reinikka, R. and J. Svensson, 2006. *The Returns from Reducing Corruption: Evidence from Education in Uganda – Revised May 2007*. http://www.qog.pol.gu.se/qog_course/readings/TestingJune2007%20Svensson%20Reinikka.pdf

Shleifer, A. and Vishny, R. W. , 1993, Corruption, *The Quarterly Journal of Economics* 108(3): 599–617.

Svensson, J., 2005, Eight Questions about Corruption, *Journal of Economic Perspectives* 19(5): 19–42.

Tanzania Communications Regulatory Authority (TCRA), 2010. *Telecommunications Statistics from 2000 to December 2009*. http://www.tcra.go.tz/publications/telecom.html (2010-05-30)

Textually, 2006. *Bribe Recorded on a Mobile Phone*. http://www.textually.org/textually/archives/2006/05/012276.htm

The Economist, 2009. *Mobile Marvels: A Special Report on Telecoms in Emerging Markets*. 26 September 2009. http://www.economist.com/specialreports/displayStory.cfm?story_id=14483896

Transparency International Uganda (TIU), 2007. *Tackling Corruption: A Reference Handbook for Anticorruption Activists in Uganda*. Dual Trust Designers.

Transparency International (TI), 2010. *Corruption Perceptions Index*. http://www.transparency.org/policy_research/surveys_indices/cpi/2009

United Nations Development Programme (UNDP), United Nations Office on Drugs and Crime (UNODC), 2009. *Corruption. A crime against...* www.yourno-counts.org

Verclas, K., 2010. *Scaling Mobile Services for Development: What Will It Take?*. http://mobileactive.org/scaling-mobile-services-development-what-will-it-take)

World Bank, 2010. *Africa Development Indicators 2010: Silent and Lethal: How Quiet Corruption Undermines Africa's Development Efforts*. http://siteresources.worldbank.org/AFRICAEXT/Resources/english_essay_adi2010.pdf

World Bank Group, 2009. *Governance Matters 2009, Worldwide Governance Indicators (WGI) 1996-2008*. http://info.worldbank.org/governance/wgi/pdf/wgidataset.xls

World Bank Institute, 2010. *Cell Phones and Radio Counter Corruption in Burundi*. http://wbi.worldbank.org/wbi/stories/cell-phones-and-radio-counter-corruption-burundi

Zuckerman, E., 2009. *A Response to "A Dialogue on ICTs, Human Development, Growth and Poverty Reduction".* Blogpost 18 September 2009. http://publius.cc/response_dialogue_icts_human_development_growth_and_poverty_reduction/0917_0

Interviews

John Silco Muragahara, RIC-NET. 21 September 2009.

Jasper Tumuhibise, Lantern Consulting. 7 December, 2009.

David Turahi, Ministry of Information and Communication Technologies. 8 December 2009

Aaron Mukwaya, Makerere University, 17 December, 2009.

Christine Mugimba, Manager-Research and Development, Uganda Communications Commission (UCC). 17 December, 2009.

Internet Cencorship Challanged
- How Circumvention Technologies Can Effectively Outwit Governments Attemts to Filter Content. Alkasir, a case study.

Walid Al-Saqaf

Unlike studies on censorship in speech, art, film, print and broadcast media, there has been little academic research on censorship of dissident content on the Internet, and the subject that has received even less attention in this field is the emerging phenomenon of censorship circumvention technologies. This study attempts to prove that censorship circumvention techniques are able to challenge Internet censorship of dissident content. This comes at a time when censoring online content critical of governments has reached high levels, particularly in regions witnessing unprecedented growth rates in Internet use, e.g., China, Iran and Arab countries. The paper makes the case that there are technological means to bypass Internet filtering of dissident content and such means are efficient and affordable. To demonstrate this point, the paper presents a case study of the "alkasir" circumvention solution for the period from July 2009 to May 2010. The study

concluded that users of alkasir, particularly in the Middle East, have used the program during this time to access websites containing dissident content that would otherwise have been filtered.

INTRODUCTION

It is estimated that almost 2 billion persons, which represents about 29% of the world's population, have access to the Internet, as of 2010 (Internet Usage World Stats, 2010). Those numbers are expected to increase rapidly in the coming years as Internet connectivity will be more commonly available on mobile phones, which would increase the number of Internet users to over 2.7 billion persons, i.e., a third of the world's population, by 2013 (Tsai, 2009). Apart from the rise in the number of users, the functions and online services[i] offered will also increase due to new innovations in software and infrastructure, raising the annual global Internet traffic to two-thirds of a zettabyte[ii] by 2013 (Cisco, 2009).

Along with this rapid growth in Internet use, the phenomenon of Internet censorship has also become increasingly visible. The subject of Internet censorship has started to garner attention by scholars and research institutions in different disciplines including media and communications, information technology, law, political science, and economics. Reports dealing with Internet censorship have also been produced by advocacy groups such as the Paris-based Reporters without Borders and the Washington DC-based Freedom House.

Internet censorship is a rather complex subject as it is comprised of several aspects that have to do with the Internet's structure and application, Internet users' behaviour, state control, along with several other factors that vary based on the socio-economic and political situations in the country in question. Unlike censorship in other areas[iii], Internet censorship is a relatively new phenomenon and remains seriously under-researched. It is important to bring this subject to the

forefront of ICT studies because Internet censorship has been a rising trend in recent years not only in the Arab world, but in Iran, China, South East Asia and to a limited degree, in Africa, as will be described below. Although censored content varies widely based on country, culture and context, and may range from child pornography to gambling, this essay is primarily concerned with censorship of dissident content. Here, *dissident* refers primarily to government-critical content and messages that challenge the established concepts or ideas in a specific country or culture. In order to understand Internet censorship of dissident content, it is important first to understand Internet censorship in terms of definition and implementation.

Given that the study focuses on filtering of dissident content as the main technical method of censorship, the words *censorship* and *filtering* may be used interchangeably throughout the remainder of the study unless implied otherwise. Hence, when describing *censorship circumvention*, it is to be understood as *the bypassing of dissident content filtering*.

Furthermore, as will be described in the methodology section, the sample selected for the study constituted of alkasir users in the Middle East and North Africa. The study analysed the use of alkasir for over seven months and compiled important statistics verifying that users were indeed able to access dissident content that was blocked from access through regular means.

PURPOSE

The study's main goal is to demonstrate that Internet censorship can be challenged through the use of technology. In other words, the study's goal is to answer the question: How can Internet users use circumvention technologies to access dissident content from which they are otherwise blocked?

The hypothesis that the study attempts to prove is: Internet users can render censorship largely ineffective through the use of technology. It is important to emphasize at this point that the study does not go beyond *dissident* content vis-à-vis content that is censored for various other reasons (e.g., pornography, terrorism, etc.). It is also not the purpose of this study to prove that circumvention of such censorship is beneficial or necessary for society, which is a more challenging – and arguably more appealing – topic of research.

The study's contribution here is as a pioneering initiative, attempting to generate and analyse the empirical evidence necessary to prove that technology can indeed be used efficiently to circumvent censorship effectively. It does so by presenting the first detailed analysis of a case study of a technological solution used to challenge Internet censorship imposed by Internet service providers (ISPs) on their users. That case study was confined to the use of *alkasir*[iv], a circumvention solution developed by the author based on a technology that is currently under development and mainly aims at circumventing censorship of dissident content while tracking censorship patterns of such content globally and nationally. A detailed description of how alkasir works and how it allows users to bypass Internet censorship of dissident content is presented in a later section.

PREVIOUS STUDIES

I did not find any previous studies dedicated to circumvention technologies of censorship. However, there were several studies on Internet censorship and particularly on the *filtering* of online content. Filtering is the focal point of a significant number of studies (e.g., Al-Hajery and Eyas, 2000; Deibert, Palfrey, Rohozinski and Zittrain, 2008; Heins, Cho and Feldman, 2006; Zittrain and Edelman, 2003; Peltz, 2002). Other studies, on the other hand, focused on non-technical means of censorship, such as the use of force and intimidation through threats, beatings, prosecutions, offline surveillance and similar

policies that targeted online journalists, bloggers and cyber activists. An overall conclusion was that such acts contribute greatly to increasing the level of self-censorship (Freedom House, 2009; Reporters without Borders, 2006).

Earlier studies on Internet censorship mostly focused on a particular country or region. China has been the subject of the vast majority, being targeted by many researchers and institutions based in the United States and Europe (e.g., Cain, 2009; MacKinnon, 2008; MacKinnon and Human Rights Watch, 2006; Menon, 2000; Palfrey, 2009; Wacker, 2003; Zittrain and Edelman, 2003). There was also literature focusing on Internet censorship in the Middle East (e.g., Zarwan, Goldstein, Ghaemi, Stork, PoKempner, and Saunders, 2005) and other countries such as Iran (Mina, 2007), Singapore (e.g., Hwa and Berlinda, 1996), the United States (e.g., Ebbs, Geoffrey and Rheingold, 1997; Maines, 1996), Australia (e.g., Simpson, 2008), the United Kingdom (e.g., Brett, 2009), the Netherlands (e.g., Stol, Kaspersen, Kerstens, Leukfeldt, and Lodder, 2009) and Thailand (e.g., PaireePairit, 2008).

Research carried out by the Open Net Initiative (ONI) found that in Sub-Saharan Africa, while the region has a history of restrictions on the media and freedom of the press, ironically Internet filtering is not practised except for one country: Ethiopia. Beyond the study by ONI, no studies were found to have focused on the different forms of censorship.

The low level of Internet filtering in Africa was attributed to the poor infrastructure, as only 17% of Africans have an electricity supply, with this percentage dropping to 5% among the rural population (Open Net Initiative, 2010). Consequently, Sub-Saharan Africa has a very low Internet penetration rate, averaging 5.59%, as of 2008, and ranging from 0.25% in Sierra Leone to 40.44% in the Seychelles[v]. Nonetheless, and apart from Ethiopia, which was found to be censoring independent media, blogs, and political reform and human rights sites, there were measures taken by several African governments, such as Cote d'Ivoire, Ethiopia, Botswana, Malawi and Ghana

to restrict Voice over Internet Protocol (VoIP) services (Open Net Initiative, 2010).

To understand how alkasir was used to circumvent Internet censorship, it is important first to reflect on how earlier studied defined how Internet censorship works. To do so, we ought to start with the Internet, which is defined as "a worldwide system of interconnected computers and computer networks that use the TCP/IP protocol suite"[vi] (Perritt, 2010), then one can argue that censoring the Internet involves limiting connectivity of its users to the rest of the Internet. Censoring the Internet is unlike censorship of traditional broadcast or print media because the Internet is not a medium of communication per se, but is rather a distributed network with interactive capabilities that could also serve as a collection of media with content generated and used by people for very different reasons (Cannon, 2001:32).

In his book, *The Internet Galaxy*, Castells emphasized the difference between conventional media and the Internet by using the title "Opening: The Network is the Message"[vii] for his preface. It was a mimicry of Marshall McLuhan's phrase "The medium is the message" . Castells used network instead of medium to stress that the Internet is in fact a network (Castells, 2003:1) and that is what allows it to have vast capabilities that could be utilized by users in many ways.

Furthermore, because the Internet is a distributed network, it is difficult to control and govern by any single entity because its components are owned by millions of users around the world. With this in mind, it appears that there is no definition of Internet censorship at hand. This opens a window of possibilities to formulate a formal definition that could serve as a breakthrough in this field at this level and which happens to be one of the aims of my future research. However, to do so, it is essential to understand the mechanisms of Internet censorship.

Internet Censorship Mechanisms

Hersberger (2004) presented several mechanisms of Internet censorship, including the use of filtering software, which can block websites from access by Internet users on a certain level. Filtering can take place on the computer level or on an intranet level through network administrators and ISPs, in which case, only the portion of users who connect to the Internet through those layers will not be able to view the content (Hersberger, 2004: 266). If the state monopolizes all ISPs, then censorship would be on a national level. Filtering is the most common method used by ISPs to implement technical Internet censorship and it is what alkasir is able to circumvent, as shall be described later.

C. Grothoff, Horozov, Lindgren and Krista (2003:1) noted that Internet censorship is a "weapon" used to suppress the dissemination of information and to stifle dissent. They noted that censorship on the Internet could be done in a number of ways including filtering and denial-of-service (DoS) attacks, as well as through harassment of those who publish information online (Grothoff et al., 2003).

In a report published by Human Rights Watch, Zarwan, Goldstein, Ghaemi, Stork, PoKempner, and Saunders on Internet freedom in the Middle East, the authors used the term *cyber censorship* and referred to various forms of such censorship including filtering, legal restrictions, threats, intimidation and surveillance (Zarwan et al., 2005).

Murdoch and Anderson (2008) described in detail the different methods and tools used in Internet filtering, which ranged from technical filtering to domain deregistration and DoS attacks. They also briefly touched upon surveillance and non-technical censorship methods (Murdoch and Anderson, 2008:65).

The authors described the main methods of Internet censorship as follows:

(Murdoch and Anderson, 2008: 59-65)
(1) TCP/IP header filtering: With this method, the censor's router can inspect the Internet Protocol [IP] address[viii] and port number[ix] of the destination. If the destination is found to be on a blacklist, the connection is dropped or redirected to a page indicating that access to the destination is denied. Such a measure may result in over blocking because some servers use the same IP address for different website addresses.

(2) TCP/IP content filtering: This is a similar method to header filtering except that the censor's router inspects the packet contents for any patterns or keywords that may be blacklisted. This method is rather complex and resource hungry.

(3) Domain Name Server (DNS) Tampering: Normally, domain name servers are accessed by user computers to retrieve the corresponding IP address of a given domain. Through DNS tampering, domain name resolution could fail as the router could send back an erroneous response that does not contain the right IP address, hence the connection fails.

(4) Hyper Text Transfer Protocol (HTTP) Proxy Filtering: In some cases, users are forced to use HTTP proxies that are assigned for accessing the Internet. Those proxies may be the only way to reach the Internet and hence they can monitor all traffic that goes through them. Such a method is more powerful than TCP/IP header and DNS filtering.

(5) Hybrid TCP/IP and HTTP Proxy: Because using HTTP Proxy Filtering is often demanding, a solution was devised to use only HTTP Proxy filtering for a list of IP addresses known to have prohibited content. If any of those IP addresses is accessed, traffic is redirected to a transparent HTTP proxy, which inspects the transferred stream and filters any banned content.

(6) Denial of Service (DoS): In addition to conventional blocking mechanisms, what is known as a DoS attack could be launched on the host server. Such attacks are usually done by having a large number of computers requesting service from a particular server and hence, overwhelming it with too much traffic which causes the server and its connection to stall.
(7) Server Takedown: Through legal, extra-legal or pressure methods, a company hosting a specific server could take it down and disconnect it from the Internet. The owner of the server may be able to transfer the server's contents, however – provided that a backup copy existed – to another hosting company within hours.

(8) Surveillance: Constant technical monitoring through logging transfers between the host and the Internet user. If banned content is found in the transferred stream, actions – legal or extra-legal – could be taken against the user, the host or both. Such acts could trigger a sense of fear, causing the host to refrain from publishing such content and causing the user to hesitate from accessing it.

(9) Social techniques: Apart from technical methods ranging from filtering to surveillance, social methods were also applied. Among them was the requirement to show a photo ID before using public computers at libraries or Internet cafés. Social or religious norms that force Internet users to avoid opening particular content are another form of social censorship.

Similarly, Zittrain and Palfrey (2008:2) focused on the technical filtering aspect of Internet censorship. They defined filtering as the "technical blockage of the free flow of information across the Internet". They also complemented the work of Murdoch and Anderson by describing in greater detail the legal and social measures used in Internet censorship. One of such measures they identified was self-censorship, which is practised by online discussion forum moderators, who often remove contributions that could lead to the blocking of their websites (Zittrain and Palfrey, 2008a:42).

Although Internet censorship goes beyond filtering, as emphasized in a number of studies (e.g., Deibert and Rhozinski, 2008; Freedom House, 2009; Reporters without Borders, 2009; Zarwan et al., 2005), this study is confined to Internet filtering, which Open Net Initiative[x] refers to as "technical approaches to control access to information on the Internet" (Open Net, 2010a). The case study of alkasir is centred around its ability of circumventing Internet filtering or more specifically, the first two methods mentioned above, namely: TCP/IP header and content filtering. The next section describes how alkasir can technically bypass such censorship.

RESEARCH METHOD

The methodology used for the study is purely empirical as it relies solely on the data gathered from alkasir's server storage. *Quantitative content analysis* was applied to derive and analyse statistics based on the information that was logged on a specific hard disk for many months. This information includes the times and data users received or sent to the proxy server of alkasir through the client-based application that is installed on the user's personal computer (Windows OS-based).

Alkasir became fully operational in July 2009, just about two months after its official launch.[xi] More precisely, the log data available was collected in the period from 17 July 2009 to 30 May 2010. This sample is rather large and is taken in the strata as a whole without any exceptions or gaps so as to generate the least possible sampling variance and error.

Stratified sampling was used for the study by selecting a subset of Internet users of censorship circumvention solutions from all the Internet users. Within this subset, only those using alkasir were chosen. It is assumed that users of alkasir share the common characteristic of being individuals seeking to access websites filtered – often because of their dissident content – by their Internet Service Provider (ISP). Alkasir differs from other similar solutions in that it only allows access to a spe-

cific type of content based on a clear policy.[xii] This sampling approach was chosen because it is convenient due to accessibility of logged information on alkasir's server and because such a sampling method is superior to random sampling in terms of accuracy and representativity (Wilson, 1991:162).

HOW ALKASIR WORKS

Instead of describing how alkasir works in technical terms, it is perhaps more convenient to describe how it works from the user's perspective. Below is a description of how a particular alkasir user using a particular Internet Service Provider (ISP) is able to bypass a particular blocked website.

Circumvention Process

1. The user starts the software program and verifies that it is lit on the system tray.
2. The program hooks the computer to a proxy server on an external network located in a country where there is no Internet filtering through a secure tunnel.
3. The IP address of the user is used to identify the actual ISP Access Point[xiii] (ISPAP) and country information, which are discovered through geo-location software on alkasir's server.
4. The user's ISPAP entry on the database is accessed and the list of websites known to be blocked by that ISPAP is downloaded to the user's computer and integrated into an automatic configuration proxy script.
5. The user's browser (e.g., Mozilla Firefox, Internet Explorer) is set up to use the auto configuration proxy script, which in turn dynamically forwards any attempted connection to any of the blocked websites to the secure tunnel while connections to any non-blocked website go directly.

The above five simple steps are all that are needed for the user to bypass filtering of websites dynamically with alkasir. However, this process is incomplete without the ability to know which websites are in fact blocked and which ones are not. To

do this, the following steps are applied through the reporting process.

Reporting Process

1. The user finds himself/herself unable to access a website that used to be accessible in the past. That website appears to have been blocked. So he/she clicks a button on alkasir's interface where the blocked website's address could be fed and reported as *blocked*.
2. Once the website's address is reported to alkasir's server, the content of that website is fetched locally and sent to alkasir's server to compare with the one fetched through the uncensored external server.
3. A comparison mechanism takes place on the server to verify if the website is blocked or not.
4. Once a website is verified to have indeed been filtered, it is added to the database on the server for review by a moderator.
5. Once a moderator, who is generally a volunteer coordinating with alkasir administration, approves the website and finds it in agreement with alkasir's policy, he/she marks it as accessible on the database and adds it to the list that the user downloads every time he/she starts alkasir. Once the new website is added, it is among the websites that can be reached through the tunnel as described in step (4) mentioned in the circumvention process above. Thereafter, the user is able to access the newly added website.

As explained above, the two main functions of alkasir, i.e., allowing users to circumvent censorship and to report blocked websites, complement each other. Every time a new website is reported by a single user and approved by a moderator, that website becomes accessible by all alkasir users using the same ISPAP in that specific country. The more users use alkasir, the more likely it is that blocked websites will be reported and approved and hence the more likely that users will be able to bypass censorship.

The process of reporting a website, however, does not guarantee that the website will be approved because it should meet two basic conditions. The first is that it should be verified to be blocked and the second is that it should satisfy the policy of alkasir, which does not approve certain content such as pornography, hacking, and other types of content. Often, a reported website is not approved because it is either found to be approved already or not blocked at all. Sometimes, a website could be refused because it contains pornography or other content not allowed by alkasir's policy. This explains why only a portion of the reported website is approved.

It is important to understand that alkasir necessitates that users take the initiative in reporting about blocked websites. Otherwise, there will be no purpose in using alkasir, which is the reason why using alkasir is not productive in countries with no censorship or in countries where censorship is done for ethical or pure social reasons, e.g., pornography. Meanwhile, alkasir would be most effective in countries where dissident content is pervasively filtered (e.g., the Middle East, China).

Now that the theoretical description of how alkasir works has been explained, the next section presents the results found from analysing logs of actual alkasir users and blocked content.

FINDINGS

During the period from July 2009 and May 2010, the installation file located at http://alkasir.com that is needed to run alkasir has been accessed over 56,000 times by Internet users across the world. This does not include the times the software was fetched from external websites such as https://sesawe.net, where it is downloadable as one of the available circumvention solutions. Furthermore, this number does not necessarily indicate the number of users who used it as the same user is able to download the file more than once and there is a pos-

sibility that automated queries from search engines attempted to access the file.

For security and privacy concerns, the IP addresses of users using alkasir have been deleted from the server logs and hence it is not possible to obtain the exact number of users who used the program. However, it is possible to measure the number of times they accessed the server's database. According to the results compiled from the logs, users have come from 55 countries from the Arab world, North and South America, Europe, Sub-Saharan Africa, Asia and Oceania. Users connected to the Internet using 481 ISPAPs.

Table 1: Summary of findings

Region	Accesses	Reporting Attempts	Approved Websites
Arab World	49,214	8,352	306
Asia & Oceania	1,983	129	62
Europe	724	8	1
North & South America	926	2	0
Sub-Saharan Africa	41	2	1
Total:	**51,888**	**8,493**	**370**

Figures 1 and 2 and Table 1 summarize the main findings concerning the number of user accesses, reports attempts of blocked websites and those websites that were actually approved. As can be seen from the graphs, it was found that the Arab world dominated in all three areas with a majority of 92%, 96% and 83% respectively.

Furthermore, Figure 1 indicates that there is a positive correlation for the top 10 Arab countries between the number of user accesses to blocked websites and the number of attempts to report a website as blocked as well as the number of websites ultimately approved for access to all alkasir users.

Arab countries had the highest number of accesses and with the aforementioned positive correlation in mind, it was natural to find that Arab users had reported more websites ap-

proved than users from any other region.

Figure 1: The positive correlation between the three main variables is clearly seen for the top 10 Arab countries in the number of accesses

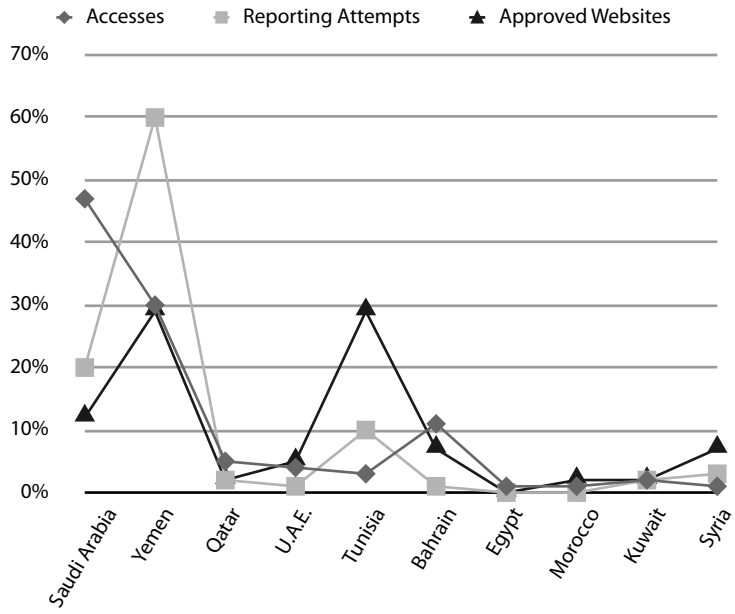

Table 2: Top 20 most accessed blocked websites using alkasir

Website	Genre	Accesses	Countries blocking it
yemenportal.net	Aggregator with dissident content	228,815	Yemen
adenpress.com	Dissident	46,260	Yemen, Saudi Arabia
tagged.com	Social Networking	39,750	Yemen Saudi Arabia
sadaaden.com	Dissident	36,281	Yemen
alkasir.com	Circumvention	16,986	Yemen, Saudi Arabia
al-teef.com	Dissident	20,565	Yemen
siutakgnoub.com	Dissident	16,420	Yemen
youtube.com	Multimedia Sharing	12,663	Tunisia, Syria, Sudan, Iran, Turkey, China, Bahrain
al-yemen.org	Discussion Forum with dissident content	11,753	Yemen
facebook.com	Social Networking	8,595	Syria, Iran, China, Pakistan, Bahrain
almenpar.info	Dissident	7,601	Yemen, Saudi Arabia
adengulf.net	Dissident	7,251	Yemen
tajaden.org	Dissident	7,197	Yemen
almasdaronline.com	News with dissident content	6,277	Yemen

Website	Genre	Accesses	Countries blocking it
al-ayyam.info	News with dissident content	3,990	Yemen
bbc.co.uk	International News	3,937	Iran
dhal3.com	Discussion Forum (dissident)	3,848	Yemen
4shared.com	Multimedia sharing	3,700	Yemen, China
siyasapress.net	Dissident	3,366	Yemen
al-tahreer.net	Dissident	3,016	Yemen

In essence, alkasir was launched as an Arab initiative when it was publicly announced at an international seminar held in Cairo on 15 May 2009. It was declared to be a project aimed at introducing a circumvention solution that could be used by Arab users willing to evade censorship imposed on dissident content. Unlike other internationally renowned circumvention solutions at the time, alkasir was not intended to be used to access content that was censored due to reasons deemed socially inappropriate in Arab and Muslim countries, such as pornography. Hence, it was believed that this solution could be more acceptable and welcomed in those countries compared with other solutions that allowed circumvention of all websites regardless of their content.

Secondly, the marketing of alkasir was mostly done in a few Arab countries, such as Egypt, Yemen, and Saudi Arabia. It was widely advertised on YemenPortal.net and reported more visibly in Arabic-speaking websites.

Blocked Websites

Arguably, the most important finding of the study is the popularity of the blocked websites that users actually accessed.

The study identified the 20 most frequently accessed websites and classified them according to genre and countries where they were blocked.[xiv]

Expectedly, the most frequently accessed sites were those blocked in the countries where alkasir is most widely used, i.e., Yemen and Saudi Arabia. Table 2 verifies this as almost all the top 20 websites are blocked either in Yemen, in Saudi Arabia or in both.

There were, however, a few exceptions. Among the websites in the top 20 list are youtube.com and facebook.com, both which are not blocked in Yemen or in Saudi Arabia. However those two websites may have made it to the top 20 list because of their combined accesses from several countries that are filtering them. Although those websites do not carry dissident content per se, they can potentially be used to convey and share dissident views through the use of features such as videos and discussion forums.

Figure 2: Accesses distribution based on genre for the top 20 websites

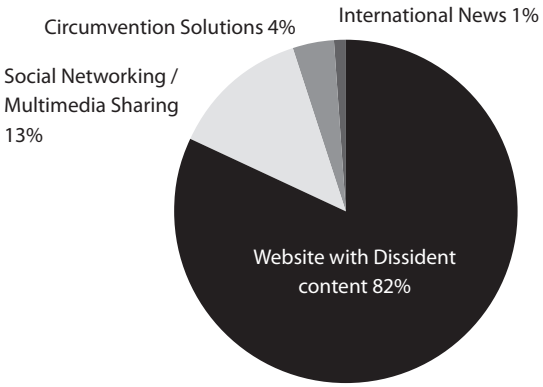

Figure 2 is perhaps the most important graph of the study as it points to the fact that 82% of accesses to the top 20 websites were aimed at websites that included dissident content, which was blocked from their access by their ISP. The fact that 13% of the access went to social networking and multimedia sharing websites where dissident content can also exist, only confirms the study's hypothesis. In other words, alkasir, a circumvention technology, did indeed allow users to access dissident content and has in fact outwitted government censorship through the use of technology.

CONCLUSION

The study presents a detailed and in-depth look at how technology could be used to circumvent censorship for Internet

users so as to allow them access to dissident content from which they would otherwise be blocked from accessing by ISPs. The findings obtained from analysing the log files of over seven months-worth of data showing the activity of users of the alkasir circumvention solution have demonstrated that the users were in fact able to bypass censorship and read dissident content from which they were banned through regular means.

Although the main beneficiaries of alkasir appeared to be Arab Internet users particularly in Yemen and Saudi Arabia, its potential in becoming a global viable circumvention solution was demonstrated by Chinese, Iranian and other netizens who used alkasir to reach social networking and multimedia sharing websites such as facebook.com and youtube.com. This signals the possibility for circumvention technologies in general to serve multiple purposes; firstly in allowing users access to and the ability to publish dissident content on websites otherwise blocked by the state, and secondly, in granting them unfettered access to social networking websites, where there are services that could be utilized to create networks and find ways to disseminate and read dissident messages.

The next important step to take when researching circumvention technologies is to look into ways to expand the number of users of such solutions to gain a better understanding of where, why and how such tools could be used. This will help bring greater light to the rather mysterious and largely unexplored area of Internet censorship circumventions.

REFERENCES

Al-Hajery, Eyas S. (2000) *Evaluating Web Filters: A Practical Approach*. http://www.isoc.org/inet2000/cdproceedings/8k/8k_5.htm (10 March 2010)

Brett, Alastair (2009) 'Law warp'. *Index on Censorship*, 38(2): 89-95.

Cain, G. (2009) 'The cyber-empire strikes back'. *Far Eastern Economic Review*, 172(2), 50-52.

Cannon, Hugh M. (2001) 'Addressing new media with conventional media planning'. *Journal of Interactive Research* 1(2).

Castells, Manuel (2001) *The Internet Galaxy, Reflections on the Internet, Business and Society*. Oxford, Oxford University Press.

Cisco (2009) *Hyperconnectivity and the Approaching Zettabyte Era*. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.html (10 March 2010).

Deibert, R. J. and Rohozinski, R. (2008) 'Good for liberty, bad for security? Global civil society and the securitization of the Internet' in R. J. Deibert, J. G. Palfrey, R. Rohozinski, and J. Zittrain (Eds.) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, R. J., Palfrey, J. G., Rohozinski, R. & Zittrain, J. (Eds.) (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Ebbs, Geoffrey and Rheingold, Howard (1997) 'Censorship on the information highway'. *Internet Research*, 7(1): 59-60.

Freedom House (2009) *Freedom on the Net: A Global Assessment of Internet and Digital Media*. http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTheNet_FullReport.pdf (10 March 2010)

Grothoff, C., Horozov, T., Krista, B, and Lindgren, J. T. (2003) *An Encoding for Censorship-Resistant Sharing*, Technical report http://www.cs.helsinki.fi/u/jtlindgr/stuff/ecrs.ps.

Heins, Marjorie, Cho, Christina and Feldman, Ariel (2006) *Internet Filters: A Public Policy Report*, 2nd edn, Washington, DC: Brennan Center for Justice.

Hersberger, J. A. (2004) 'Internet censorship'. In Hossein Bignoli (Ed.), *The Internet Encyclopedia*, 2: 264-274. Hoboken, NJ: John Wiley and Sons.

Hwa, Ang Peng and Berlinda, Nadarajan (1996) 'Censorship and the Internet: A Singapore perspective'. *Association for Computing Machinery. Communications of the ACM* 39(6): 72-79.

Internet Usage World Stats (2010) http://www.internetworldstats.com/stats.htm (24 August 2010).

MacKinnon, Rebecca (2008) 'Flatter world and thicker walls? Blogs, censorship, and civic discourse in China', *Public Choice*. 134 (January): 31-46.

MacKinnon, Rebecca, and Human Rights Watch (Organization) (2006) 'Race to the Bottom': *Corporate Complicity in Chinese Internet Censorship*. New York: Human Rights Watch.

Maines, Patrick D. (1996) 'The new censorship'. *Editor & Publisher*, 129(37): 48.

Menon, K. (2000) 'Controlling the Internet: Censorship online in China'. *Quill*, 88(8): 82.

Mina, N. (2007) *Blogs, Cyber-Literature and Virtual Culture in Iran*. Washington, DC: Storming Media.

Murdoch, Steven J. and Anderson, Ross (2008) 'Tools and technology of Internet filtering', in R. J. Deibert, J. G. Palfrey, R. Rohozinski, & J. Zittrain (Eds.) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Open Net Initiative (2010a) *Sub-Saharan Africa* http://opennet.net/research/regions/ssafrica (11 June 2010).

Open Net Initiative (2010b) *About Filtering* http://opennet.net/about-filtering (30 May 2010)

PaireePairit, Isriya (2008) *Internet Censorship in Thailand*, MSc. Thesis, Department of Information Management, The University of Sheffield, Sheffield, England.

Palfrey, J. (2009) 'Internet Arms Race'. Technology Review, 112(3): 10-11.

Peltz, Richard J. (2002) 'Use the filter you were born with: The unconstitutionality of mandatory internet filtering for the adult patrons of public libraries'. *Washington Law Review*. 77: 397-480.

Perrit Jr., Henry H. (2010) *What is the Internet?* http://www.kentlaw.edu/cyberlaw/resources/whatis.html (10 March 2010).

Reporters Without Borders (2006) *List of the 13 Internet Enemies* http://www.rsf.org/List-of-the-13-Internet-enemies.html (10 March 2010).

Simpson, B. (2008) 'New Labor, new censorship? Politics, religion and internet filtering in Australia'. *Information & Communications Technology Law*, 17(3): 167-183. doi:10.1080/13600830802472982.

Stol, W.P., Kaspersen, H.K.W, Kerstens, J., Leukfeldt, E.R. and Lodder, A.R. (2009) 'Governmental filtering of websites: the Dutch case'. *Computer Law and Security Report*, 21(3): 251-262.

Tsai, Joseph (2009) 'Number of mobile devices accessing the Internet expected to surpass 1 billion by 2013, says IDC'. http://www.digitimes.com/news/a20091210PR204.html (10 March 2010).

Wacker, Gudrun (2006) 'The Internet and censorship in China', in Hughes, Christopher R. & Wacker, Gudrun (Eds.), *China and the Internet: Politics of the Digital Leap Forward*. London, England: Routledge.

Wilson, Edgar (1991). *An Introduction to Scientific Research*. New York: Dover Publications.

Zarwan, E., Goldstein, E., Ghaemi, H., Stork, PoKempner, D. J. and Saunders, J. (2005) 'False freedom: Online censorship in the Middle East and North Africa'. *Human Rights Watch*, 17(10-E): 1-116.

Zittrain, Jonathan and Edelman, Benjamin G. (2003) 'Internet filtering in China'. *IEEE Internet Computing*, March/April: 69-77. doi:10.2139/ssrn.399920.

Zittrain, Jonathan and Palfrey, John (2008a) 'Introduction' in R. J. Deibert, J. G. Palfrey, R. Rohozinski, and J. Zittrain (Eds.) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Zittrain, Jonathan and Palfrey, John (2008b) 'Internet filtering: The politics and mechanisms of control" in R. J. Deibert, J. G. Palfrey, R. Rohozinski and J. Zittrain (Eds.) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Notes

[i] The authors predict that the increase will mostly be in the use of the Internet for business and multimedia communication and entertainment, including but not limited to video conferencing, video sharing, motion pictures, online gaming, virtual words, Internet TV, 3D video, home theatre, imaging, mobile phone applications, trusted computing, peer-to-peer, and remote backup of data.

[ii] A zetta corresponds to 1027 (10 to the power of 27).

[iii] There are several studies that deal with censorship of speech, art, print and broadcast media, films, theatrical plays, photography and news reports.

[iv] Alkasir means "the circumventer" in Arabic. The software is currently downloadable at https://alkasir.com. It is a trademark registered by the Swedish Patent and Registration Office.

[v] Statistics produced dynamically through the International Telecommunication Union Dynamic Reporting service at http://www.itu.int.

[vi] The TCP/IP stands for the Internet Protocol Suite, which is a set of standard protocols that are used on the Internet and other similar networks.

[vii] Marshall McLuhan introduced the phrase "The medium is the message" in his 1964 book Understanding Media: The Extensions of Man. He attempted to show that the form of the medium can affect the way the medium is understood by audiences by embedding itself in the message.

[viii] Every computer connected to the Internet must have an IP address, which can be used to identify the Internet service provider and the geo-location of the user.

[ix] A port is an application-specific construct used to identify the service or application that is required by the requesting Internet application

[x] The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto;

the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa).

[xi] See an article about the official launch here: http://www.yementimes.com/DefaultDET.aspx?i=1260&p=local&a=2.

[xii] Alkasir does not allow bypassing censorship of pornography and some other types of content. The policy of what alkasir allows to be tunneled is accessible online at: https://alkasir.com/policy.

[xiii] An ISP access point is defined here as the name that the ISP assigns in the global geo-location database for a particular IP subset. It could be to a name for a specific wireless connection point, the name of a particular university network, a name for a mobile company's access node, etc.

[xiv] Note that the blocked websites refer to their status at the time they were reported blocked by a user and were marked as blocked on the server of alkasir. They may have been unblocked later and may well be currently not blocked in the respective countries.

About the Authors

Åke Grönlund is (full) Professor of Informatics at Örebro University, Sweden. Åke's research concerns the use of information and communication technologies (ICT) in various human activities. The common denominator involved in all projects is to understand how people arrange their work, their organizations, and other activities pertaining to private life, such as socializing on the web, and how ICT can be used for improvements. eGovernment and ICT for Development are two strong foci.

Rebekah Heacock has a Master of International Affairs from the Columbia University School of International and Public Affairs and is currently a Project Coordinator at Harvard's Berkman Center for Internet and Society (http://cyber.law.harvard.edu). Rebekah is Co-Director of the Technology for Transparency Network (http://transparency.globalvoicesonline.org), which is a project of Global Voices Online, an international community of bloggers who report on blogs and citizen media from around the world (http://globalvoicesonline.org).

Johan Hellström is a PhD student at the University of Stockholm, where he is researching how ICT and in particular mobile phones, can improve transparency, accountability and participation. He also runs the company UPGRAID (www.upgraid.com), which undertakes consultancies in the ICT4D field. Prior to beginning his PhD studies, Johan worked as an ICT4D Advisor at the Swedish International Development Cooperation Agency and as a coordinator at the Uppsala Centre for Sustainable Development.

Walid Al-Saqaf is a PhD candidate at Örebro University, Sweden, and a lecturer at School of Humanities, Education and Social Sciences. He is the inventor of the alkasir circumven-

tion solution https://alkasir.com, which allow for individuals to circumvent Internet censorship. Walid is also founder and manager of the Yemen Portal http://yemenportal.net), which aggregates news and multimedia content related to Yemen from multiple sources of different political affiliations. Before pursing his post-graduate studies in Sweden, he was the editor-in-chief of Yemen Times during 1999-2005.

Information and Communication Technology (ICT) can support democracy and human rights by expanding citizens' opportunities to participate in political decision-making, by providing citizens with access to information, and facilitating dissemination of information, as well as enabling social mobilization. A better informed citizenry who can put pressure on national institutions to be accountable and responsive to citizens' needs and priorities is a fundamental component of a functioning democracy. ICT can also improve the public sector's coordination capacity and service delivery by employing user-friendly administrative systems and appropriate Knowledge Management systems. Lastly, ICT has a real potential to prevent and should it occur, expose corrupt practices.

This anthology presents articles on how ICT can increase transparency and fight corruption.

ICT and corruption – theory and practice
Åke Grönlund

ICT4 Transparency in Sub-Saharan Africa
Rebekah Heacock & David Sasaki

Mobile Technology as a means to fight corruption
Johan Hellström

Internet censorship challenged
Walid Al-Saqaf

The Swedish Program for ICT in Developing Regions - SPIDER - is a network organisation working with ICT in health, governance and entrepreneurship in low-resource settings.

Stockholm University

SPIDER is hosted by Department of Computer and System Sciences at Stockholm University

ISBN 978-91-85991-02-0