Journal of Information Technology (2012) 00, 1–17
© 2012 JIT Palgrave Macmillan All rights reserved 0268-3962/12
palgrave-journals.com/jit/

Research article

Internet censorship circumvention technology use in human rights organizations: an exploratory analysis

Carleen Maitland[1], H F Thomas III (Trey)[2], Louis-Marie Ngamassi Tchouakeu[1]

[1]College of Information Sciences & Technology, Penn State University, University Park, PA, USA;
Q1 [2]Department of Government, University of Texas at Austin, Austin, TX, USA

Correspondence:
C Maitland, College of Information Sciences & Technology, Penn State University, 102J IST Building, University Park, PA 16802, USA.
Tel: +1 814 865 8952;
Fax: +1 814 865 2174;
Q2 **E-mail: cmaitland@ist.psu.edu**

Abstract
Using an organizational informatics approach, this study explores the implications of human rights organizations' use of censorship circumvention technologies. Through qualitative analyses of data collected through in-depth interviews, the research examines the factors influencing the use of circumvention technologies and the organizational effects of their use. The outcomes include a revised model of censorship circumvention technology use as well as a new model situating human rights organizations and their audiences in bidirectional information flows. The research provides recommendations for practice as well as insight for organizational informatics and information systems security research in the areas of protective technologies, awareness, detection, and physical security.

Journal of Information Technology (2012) **0,** 1–17. doi:10.1057/jit.2012.20
Keywords: internet censorship; human rights organizations; censorship circumvention technologies; organizational informatics

Introduction

Increasingly nation states act to restrict information flows, including restricting access to potentially subversive online information, filtering messages of dissent or preventing the spread of independent information. While the Chinese government has a well-known and enduring program of Internet censorship, governments also engage in sporadic or just-in-time censorship as was observed in the 2011 Arab uprisings (Zittrain and Edelman, 2003; Deibert *et al*., 2008, Deibert *et al*., 2010). These efforts target not only information dissemination by individuals but organizations as well, including the websites of Google and Wikipedia, world news media and human rights organizations.

International human rights organizations are particularly vulnerable to Internet censorship as their information flows include collecting difficult-to-access information about abuses as well as disseminating it to policymakers and residents of censoring countries (Rubenstein, 2004, Hopgood, 2006). This control, censorship, and regulation challenge the Internet's use as a medium for protecting human rights (Brophy and Halpin, 1999), and differentiate human rights organizations from other voluntary sector organizations, which in general successfully use the Internet carry out certain aspects of their work (Burt and Taylor, 2003).

In response, human rights organizations may find that low-cost Internet censorship circumvention technologies can secure both external information dissemination strategies and internal communications infrastructure. While estimates are difficult to make, the adoption of circumvention technologies by the general public appears to be growing. For example, Tor, a publicly available, free application that anonymizes information flows, now claims millions of users, including journalists, law enforcement, government officials, and human rights workers worldwide (see http://www.torproject.org/press/2010-09-16-ten-things-circumvention-tools.html.en). On the other hand, it is likely human rights organizations, as with all non-profits, face financial and other constraints to IT use (Corder, 2001; Saidel and Cour, 2003; Suparamaniam and Dekker, 2003), and therefore may be forced to accept censorship or use less advanced communications infrastructure.

Given these conflicting expectations, this research is a first effort to investigate the factors influencing human rights organizations' use of censorship circumvention technologies and consequences for their information flows and strategies. In particular, we examine:

1. How do the characteristics of international human rights organizations influence circumvention technology adoption and use?
2. How do the technical characteristics of censorship circumvention technologies influence their adoption and use? and,
3. How does the use (or lack thereof) of censorship circumvention technologies affect the information-related strategies of international human rights organizations?

By employing an organizational informatics approach, this research builds on previous literature that documents the important role of the Internet as an advocacy and information dissemination tool for human rights organizations. Its goal is, through the use of qualitative analyses of interview data, to provide a conceptual model that can serve as a baseline for future, more comprehensive research on censorship circumvention technology use.

This paper is structured as follows. First, the organizational informatics frame is discussed as well as various circumvention technologies and findings from the information systems security adoption literature. Next, we present a model specifying the potential technical and organizational factors influencing circumvention technology use. This is followed by a brief discussion of the research design, leading into the findings of deductive and inductive analyses. The discussion section presents a revised circumvention technology adoption model as well as a new model of human rights organizations information flows. The paper concludes with suggestions for future research.

An organizational informatics approach

This exploratory investigation requires a framework that accounts for societal as well as organizational context, provides adequate balance between the organizational and technical contexts, and accommodates multiple epistemological perspectives. Organizational informatics, as a subfield of the broader social informatics domain (Kling, 1993, 1999, 2000, 2001; Sawyer and Rosenbaum, 2000), fulfills these requirements.

The organizational and societal contexts of human rights organizations are both significant as this research investigates organizational technology adoption in response to a societal issue (censorship). Also, as compared with technologies developed exclusively for organizations (e.g. ERP systems), circumvention technologies are developed for widespread use, which may in turn influence organizational use.

Organizational informatics also provides the requisite balance between technical and organizational contexts, placing emphasis on: (1) the organizational context of ICT use and (2) the duality of influences between the organizational context and ICTs as well as consequences related to their use. Typical of organizational informatics research, our unit of analysis is the individual international human rights organization, including the dynamic consequences of IT use for organizational users, their environment, and the technology with which they interact. This duality implies both an interactive relationship in design, use, and consequences, as well as the importance of context in explaining variations in cases (Kling, 1999).

Another hallmark of organizational informatics research is recognition of the phenomenon of emergence (Markus and Robey, 1988). Inasmuch as IT architectures and organizational form and function are inextricably intertwined (Markus and Robey, 1988; Orlikowski and Robey, 1991; Orlikowski, 1993), they are mutually emergent, influenced by external, often unpredictable forces. Consequently, 'ICT use leads to multiple, and often paradoxical, effects' (Sawyer and Rosenbaum, 2000), including different effects across levels of both the organization and the ICT architecture.

Organizational informatics' explicit focus on technology is particularly valuable when studying a new and under-researched technology such as censorship circumvention tools where the range of implications is unknown. Circumvention technologies are 'configurable' in the sense that they are collections of distinct components (Sawyer and Rosenbaum, 2000). Attention to configurability helps avoid the pitfall of black-boxing the IT-artifact (Orlikowski and Iacono, 2001). This more explicit focus on technology differentiates organizational informatics from other approaches to studying duality, emergence and societal influences such as complexity theory (Axelrod and Cohen, 2000; Mitleton-Kelly and Land, 2004) and institutional theory (Scott, 1995; Lamb and Kling, 2003).

Finally, this exploratory analysis aims to provide insight for both theory and practice, combining several epistemological approaches. We develop and analyze a model of likely influences on circumvention technology use to inform theory, reflecting an analytic approach. Yet we also provide recommendations for practice, particularly in human rights organizations, reflecting a normative stance. Our approach also reflects a critical stance in our recognition of the limitations of circumvention technologies, reporting on non-technical approaches to circumvention as well (e.g. self-censorship). This combination of analytical, normative and critical approaches is typical of organizational informatics research (Sawyer and Rosenbaum, 2000).

Censorship circumvention technologies

Censorship circumvention technologies are designed to find paths to bypass restrictions on the Internet and can be used for multiple purposes, both pro- and anti-social. Human rights organizations seek clear paths for two types of information flows: (1) providing access to general human rights information as well as information about ongoing human rights abuses and (2) transfer and dissemination of that compiled information to a specific/general audience.

As depicted in Table 1, human rights organizations can use circumvention technologies for both flows. In terms of accessing information, the major problem is typically blocked access to a website (e.g. Human Rights Watch from mainland China). To overcome this problem, proxy servers, accessible through software applications, and connections through a web-based interface that use either common or unique URLs can be used. For transferring and distributing

Table 1 Censorship circumvention technologies (CCTs)

Information flow	*Strategy/technology*	*Example*
Accessing information	Proxy server/router accessed via software installed on PC	Tor, JAP, I2P
Accessing information	Web-based URL anonymizer	Common URL anonymizer; Unique URL anonymizer (Psiphon)
Distributing information	Email via anonymous remailer	Mixmaster
Distributing information	Anonymous blogging	Invisiblog
Distributing information	Use public computer	Library, Internet cafe
Distributing information	Mirroring content	Organizational partnerships

information in a way that blocks the publisher's identity, human rights organizations can make use of anonymous e-mailing (through anonymous remailers), anonymous blogging and the use public computers. If anonymity is not a concern, web postings mirrored on servers in several locations can help evade blocking.

Circumvention technologies have varied technical requirements and mixed levels of effectiveness, depending on the intended use. Circumvention tool usability may be hindered both by their added latency (Fabian *et al*., 2010) and their development by non-profit and academic research organizations, which typically lack resources for usability testing. Practical guides written by human rights and technology-related organizations provide comparative analyses and specific guidance on appropriate use.[1] These guides stipulate that many countries and organizations (schools, firms, government agencies) prohibit circumvention technology use, but also note the real risk arises from illegal dissemination of politically sensitive information.

Technical and organizational contexts

Organizational informatics requires consideration of both technical and organizational contexts. The former includes inherent technical characteristics of circumvention technologies as well as their use as information security technologies, while the latter includes the non-profit and international nature of the human rights organizations, as well as diversity in their information dissemination strategies.

Technical context

Censorship circumvention technologies can be considered information systems security technologies (Straub and Nance, 1988; Straub and Welke, 1998; Dhillon and Torkzadeh, 2006; Dinev and Hu, 2007; Zafar and Clark, 2009), bearing similarities to those used in commercial contexts. For example, the technologies and strategies used to mitigate website blocking may be similar to those for a denial of service attack, as both attacks seek to restrict information dissemination.

In the IS security *adoption* literature, security technologies are denoted as 'protective,' as compared with 'negative' (harmful) or 'positive' (productivity enhancing) tools. Protective tools are designed to neutralize or disable negative technologies, and differ from positive technologies in that they provide less direct or only subtle benefits for users (Dinev and Hu, 2007). In fact, protective technologies such as anti-virus applications may actually slow system performance thereby reducing productivity.

Research on security technologies has found adoption is influenced by the trade-off between enhanced security features and other factors such as interoperability and standardization (Hernan, 2000), as well as problems with the ease-of-use (National Research Council, 2010). Also important are the degree of compatibility between the organizational task and security technology characteristics, as well as security technology complexity, which is influenced in turn by organizational capability (Carayannis and Turner, 2006).

Organizational context and information dissemination

The organizational context of human rights organizations' circumvention technology use is defined by three factors: (1) the awareness of censorship, (2) non-profit status and (3) international operations.

While IS security requires organizations pursue multiple objectives, such as sustaining an ethical workforce and ensuring data integrity, important among them is awareness (Straub and Welke, 1998; Dhillon and Torkzadeh, 2006; Dinev and Hu, 2007). In particular, awareness of security breaches, sometimes a challenge with censorship, is likely to be an important predictor of circumvention technology adoption.

Also likely to influence adoption is human rights organizations' non-profit IT environments, characterized by a lack of staff and ICT skills, operating under donor-imposed limitations through a distributed organizational structure, which in turn give rise to headquarters/field role conflicts (Maitland and Tapia, 2007). In the international context, this headquarters/field role conflict arises from the need to locate headquarters in wealthy nations with proximity to donors, while simultaneously serving clients in poor countries. Unsurprisingly, this creates challenges for implementing a uniform IT environment across the organization (Suparamaniam and Dekker, 2003).

The third element of the organizational context for the human rights organizations examined in this study is their international presence, in particular their countries of operation. Both the conditions of Internet use in a country and the legal environment, including the extent of censorship as well as penalties for circumvention technology use, may influence that use. While the United Nations establishes access to information as a basic human right, restrictions abound (Deibert *et al*., 2010), as do human

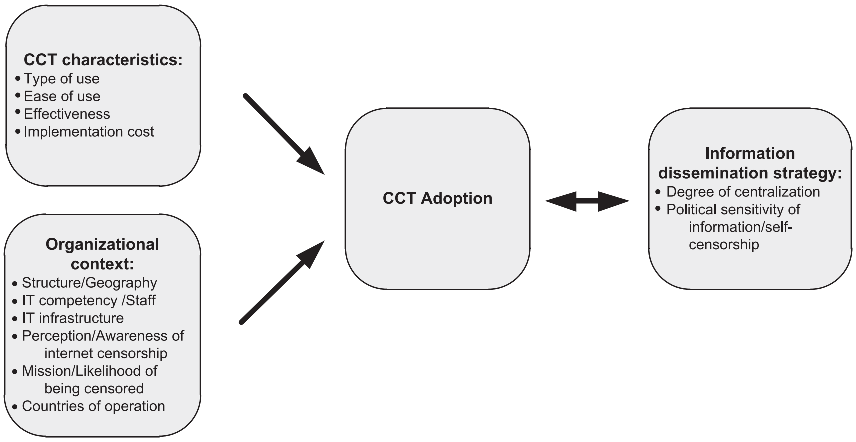

Figure 1 Model of censorship circumvention technology adoption.

rights violations perpetrated against those attempting to thwart these restrictions.

It should be noted, however, that international human rights organizations consistently work in dangerous environments where their activities put them in conflict with the law. Thus, use of circumvention technologies, even if expressly prohibited, is likely to be less of a concern than possession of the information they are trying to disseminate. Further, operations in a country may be limited to short-term information gathering expeditions, with headquarters safely located in a non-censoring country. This situation clearly does not apply to purely national organizations.

Finally, in addition to the non-profit and international context of human rights organizations, their circumvention technology use is likely to be influenced by and subsequently influence their information dissemination strategies. Human rights organizations generally seek to hold governments and other actors accountable for human rights violations, identify appropriate remedies, and proactively generate institutions that foster a respect for human rights (Rubenstein, 2004; Hopgood, 2006). Information is crucial to human rights organizations (Brophy and Halpin, 1999), particularly the large numbers employing 'naming and shaming' strategies, which require monitoring, collecting, and disseminating information.

Specifying a model of circumvention technology adoption

The above discussion suggests censorship circumvention technology use is predicted by characteristics of technical and organizational contexts, and this use both influences and is influenced by information dissemination strategies, as depicted in Figure 1. Within each of these three components, a number of variables are specified.

Drawing on the studies mentioned above, this model includes four measures of the technical characteristics of circumvention technologies: (1) type of use, (2) ease of use, (3) effectiveness, and (4) implementation cost. First, type of use relates to the information flows protected, whether incoming or outgoing. Ease of use, the second variable, reflects the difficulty, especially by inexperienced users, of configuring and using these technologies (Dingledine and Mathewson, 2006; National Research Council, 2010). Third, perceived effectiveness of circumvention technologies is included as products range in their ability to fully anonymize end-users or maintain domain visibility (Dingledine and Mathewson, 2006). Fourth and finally, while most circumvention technologies are free or open-source and do not require any up-front financial burden, the total cost of implementation (including training, hardware, and consulting expenditures) could deter even the most basic use.

The organizational variables include those both IT and non-IT related that can influence technology adoption, namely: (1) organizational structure/geography, (2) IT staff and competency, (3) IT infrastructure, (4) perception and awareness of censorship, (5) organizational mission and the likelihood of being censored, and (6) countries of activity. The first variables, organizational structure and geography, are included to measure how centralized functions and decision-making processes could influence circumvention technology adoption, which are supplemented by the second variables, the number of IT staff and their level of technical competency.

The IT environment is further represented by the level of established IT infrastructure, which could range from third-party web hosting to dedicated in-house communications technology. Also, perceptions of the threat posed by Internet censorship would likely play a significant role in decisions to implement technology to circumvent it (and vice versa), which can also be magnified or minimized by the organization's mission. Finally, the country of operations considers the likelihood of censorship and the potential affect of policies and repercussions for circumvention technology use.

In addition to the technical and organizational components, censorship circumvention technology use is likely influenced by information dissemination strategies, often a critical component in the missions of human rights organizations. However, differences among these organizations require consideration of variation in specific information dissemination strategies. Here, the degree of centralization in the information distribution decision-making structure is key since how decisions are made about the content of what goes public, as well as where and when it goes public, may potentially generate differences in the type and venue of information that is publicly distributed.

Table 2 Organizational information and server/client CCT adoption

	Informant information
	Title
Informant 1	Dir. of Communications
Informant 2	Senior Legal Counsel
Informant 3	Information Systems Coordinator
Informant 4	Dir. of Information Tech.
Informant 5	Dir. of Communications
Informant 6	Web Manager/Systems Admin.
Informant 7	Editor
Informant 8	Information Coordinator
Informant 9	Consultant to Human Rights and Technology NGOs
Informant 10	Dir. of Information Tech.
Informant 11	Former Internet Censorship Program Officer
Informant 12	Project Manager

The political sensitivity of the released information is also of note as it increases the likelihood of being a target of censorship. If an organization largely avoids posting information, either to avoid censorship or comply with sedition laws, this would likely have consequences for their need or desire to adopt circumvention technologies and vice versa. These variables are included both as independent variables with regard to the adoption and as dependent variables with regard to the effects of adoption on information flows.

Finally, circumvention technology adoption, the central factor in the model, is broad in scope as human rights organizations can utilize the technology at markedly different levels. If an organization confirms their use of any type of circumvention technology, ranging from server-side domain mirroring to simple inter-office email encryption, it is accepted that they have adopted *some* type of circumvention technology and thus are positive cases. This research, by design, also attempts to model negative cases where circumvention technologies have not (yet) been adopted. In both instances, however, this adoption or lack of adoption may be noteworthy with regard to organizational changes in information dissemination strategy and is central to the third question posed above.

Research design and data

The research employs a case study design, where the larger case of international human rights organizations' use of circumvention technologies is developed from informants from individual organizations. Identifying informants and their organizations began by coding the University of Minnesota Human Rights Library directory, a listing of 388 human rights-related organizations and their URLs, to specify a set of international organizations likely to have experience with or be directly affected by Internet censorship. A simple selection process[2] was used to separate those entries whose names indicated organizational missions or activities likely to be the target of censorship, operations in countries where Internet censorship is common, and/or operations related to issues of free expression. This baseline list of 88 organizations was supplemented by simple online search queries to locate human rights organizations specifically active on Internet censorship.

From this list, each organization's URL was visited to search for contact information preferably of staff in communications and information technology roles as well as Internet censorship/free expression campaigns or programs. General contacts or potential informants from 50 organizations were contacted via email or telephone. As individual informants agreed to participate, they were asked to provide both inside contacts to supplement their expertise and contacts to other organizations that might have experience with Internet censorship. This nested informant approach is modeled after that of Lamb and Kling (2003). The resulting variety of organizational contexts argues against potential bias developing from this approach.

Ultimately, 12 staff members from nine organizations agreed to participate in semi-structured interviews conducted between April 2008 and April 2009.[3] Tables 2 and 3 summarize informant, demographic, and interview data. The organizations interviewed are headquartered in four continents and are active in nearly all regions of the world where human rights abuses are currently ongoing. They represent a diverse population of internationally active human rights organizations as they have important variation on almost all contextual variables. Table 2 indicates the positions of the informants and Table 3 shows differences in organizational mission, staff and region-based activity, and their impact on circumvention technology adoption is described below.[4] These data represent a variety of perspectives from both the IT and communications offices of the sampled organizations, but also reflect the results of the nested interview approach which led to interviews with staff from legal and program departments as well as a third-party IT security consultant with HRO experience.

Of the nine organizations, seven operate as traditional human rights organizations, providing services directly to victims of abuses, documenting and publicly disseminating information on abuses, and/or directly lobbying government entities. The remaining two use non-traditional methods to impact human rights, such as publishing an academic journal and training other organizations in ICT.

Of the seven, three general mission types are found, namely (1) protection of individuals/stop abuse, (2) protect free expression/journalists, and (3) improve governance of human rights. These missions imply different audiences for their information. For example, while all three need to gather information on abuses, the first seeks to share that information back to potential victims, the third attempts to reach policymakers responsible for changing and implementing policies, and the second is a combination of both.

In terms of demographics, of the seven organizations, four operate worldwide, one operates in several regions, and the remaining two are regional (e.g. Asia, Europe). Their sizes range from the largest at 280 employees to just 15. As expected for non-profits and their size, their IT staffs were quite small, ranging from a high of four to zero, the latter being an indication of outsourced support. Finally, among the seven, four made use of circumvention technologies, two using both server- and client-side technologies, and two using only the latter.

Table 3 Organizational information and server/client CCT adoption

Org.	*Activities/type*	*Mission*	*Activity*	*FTE staff*	*IT staff*	*Server*	*Client*
1	Documentation	Document/stop abuses	Worldwide	280	4	Yes	Yes
2	Services	Protect individuals	Worldwide	25	**1	Yes	Yes
3	Lobbying	Seek legal reform	Asia	25	3	No	Yes
4	Services	Support local HRO	Europe/Middle East/Africa	16	*0	No	Yes
5	Services	Implement HR	Europe/Mediterranean	15	1	No	No
6	Lobbying	Protect free expression	Worldwide	30	*0	No	No
7	Services	Protect journalists	Worldwide	15	1	No	No
+8	Training	Train HR orgs in ICT	Worldwide	7	1	No	No
+9	Publishing	Publish Journal	Worldwide	1	0	No	No

Note: + Non-traditional HRO; *third-party network/web support; **third-party IT security support.

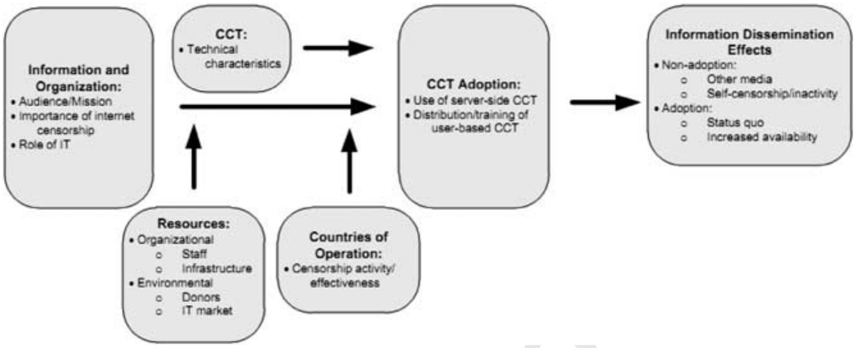

Figure 2 Revised CCT adoption conceptual model.

Analyses

The analysis includes both deductive and inductive analytic approaches. The deductive analysis investigates the relationships depicted in Figure 2, coding data from the seven traditional human rights organizations according to the scheme in Table A3 and structured around the research questions. As this research is equally concerned with adoption and non-adoption, the analysis is separated into users and non-users to help identify similarities and differences. The inductive analysis used open coding of data from all nine organizations resulting in codes indicated in Table A4.

Deductive analysis findings

How do the characteristics of international human rights organizations influence circumvention technology adoption and use?

Adopters

Among the adopters, circumvention technology use appears to be influenced by interactions between an organization's mission, the centrality of IT infrastructure and staff, and maintaining access to the organization's website.

Two of the adopting organizations have the same mission type – to monitor, document and stop human rights abuses on a broad scale. In both, the organization's website is the central method of information dissemination. One informant specifically mentions the website that also hosts a variety of email distribution lists, as the main venue for information sharing. In the second case, the emphasis placed on maintaining access to the organization's website in China and in other countries, if needed, is clear evidence of a special focus on providing publicly available information to fulfill organizational goals.

> We have about 50 email distribution lists which users can subscribe … from one per week to 10 per day and that, besides our website, [is] the main publishing method for us.
> In China, we realized that our website was likely to be blocked very easily so … we worked out a relationship where we were a part of a global coalition, which was informal and also formal, where we asked people to mirror our content and the entire report was mirrored on external websites.

In the largest organization sampled and one of two adopters of server-side circumvention technology, IT is crucial to the execution of the organization's overall mission, creating an environment conducive to adoption. IT staff are embedded in strategic planning and security functions and provide the services that enable the organization to fulfill its mission and disseminate information.

> We are the bread and soul of the organization, we live and breathe information, we don't sell anything, all we do is information, so we are looked at as strategic partners in the organization … When missions get decided on, when

> they decide on projects, we get involved early on so we can set the tempo, set the mission, set the strategic things …

Perceptions/awareness of Internet censorship is also a logical contributing factor to the implementation of circumvention technologies. One informant noted the ubiquitous organizational perception that Internet censorship is an increasingly important issue and that awareness of changes in surveillance technology must be taken into consideration.

> Everyone in the organization is aware of the limitations in freedoms … and privacy of Internet communications … We are all aware of this because we cooperate with people who are most often targeted by the surveillance systems in many different countries … and we have to know which methods and which channels of communications are better, safer, more anonymous for the given person that we cooperate with … The whole situation of surveillance is changing very fast so you can be aware of the situation at a given moment of time.

Non-adopters

Not surprisingly, a lack of IT resources and staff are the most frequently cited factors explaining a lack of organizational circumvention technology use. Even if an organization has a mission and awareness of Internet censorship that would otherwise predict adoption, some are ultimately constrained by limited resources.

In two organizations, where the web content staff remained in-house, the IT work - ranging from software support to web hosting and network administration – was outsourced. This type of arrangement, as one informant explicitly describes, creates a situation where human rights organization staff may indeed be aware of the blocking from field reports, but lack the technical knowledge and resources to initiate circumvention technology adoption.

> We just don't keep track when our website has been blocked by a country. I mean we have very limited resources to do that anyway, but I'm sure [our] website has been blocked.
>
> We have an external IT provider who we call up, who deals with any kind of Microsoft or any IT queries that we have. Our website is managed by myself, but we have an external maintainer to look after that. And then an administrative director looks after the IT, so there is not really anyone [focusing on Internet censorship] … what you are talking about falls between everyone's roles, no one particularly is designated to look after that area.

Combined, these comments by adopters and non-adopters support the influence of mission, IT infrastructure, awareness and IT competency on circumvention technology adoption.

How do the technical characteristics of censorship circumvention technologies influence their adoption and use?

As the non-adopters had little experience with circumvention technologies, here the analysis is limited to the adopters.

Adopters

Comments from informants from the four circumvention technology-adopting organizations were mostly negative in tone, especially with regard to the black-box nature of some circumvention technologies, the training costs needed to ensure proper use as well as the slow-speed of proxy servers and their inherent vulnerability.

In terms of client-side use, such as anonymous blogging or use of proxy servers, one informant described how circumvention technology use without proper training and experience can lead to breaches in anonymity that can potentially interrupt the ability of researchers to document abuses and share information. Also, while circumvention technologies are typically open-source or free services/software, the informant detailed how this need for training makes the overall implementation cost much higher than previously understood.

In terms of server-side use, a second informant describes the implementation of organization-sponsored proxy services and their inherent characteristics that make them difficult to use on a large scale. Specifically, he mentions the organization's private proxy server is too slow under load and that widespread usage would endanger access to the server itself.

> It's a huge cost for us on those, even though the software is free … but the training it requires, sometimes people have to travel, it requires resources to train, it requires handholding because the technology, if you don't know how to use it is not good. You could [have] the best lock, but if you don't know how to use it you are in trouble, so training is a big part, it's very expensive and it does cost, it's something you have to take into consideration, because if you don't use it very well, you are not secure. We have some tools to use – secure encrypted connections to proxies, which we can use and which do work, but they are slow and we cannot mass distribute that because that would harm the proxy itself and so the proxy itself would also be blocked. So we can equip staff to go into the country and get access to our website, but we have not yet made extensive use of that.

These comments reflect the role of ease of use, effectiveness, and implementation cost on circumvention technology use.

How does the use (or lack thereof) of circumvention technology affect the information-related strategies of international human rights organizations?

Adopters

Among the four users of circumvention technologies, the effects on information dissemination strategies are unclear. One informant reported their organization had implemented a strategic self-censorship practice for website content to try to minimize site blocking in China, but eventually rescinded it after seeing no change in blocking in the country. This instance is the only case of self-censorship found in the interview data. Most organizations employ unrestricted information dissemination practices. For example, two adopter informants describe a long-time organizational policy against any self-censorship. It appears, then, that circumvention technology adoption has no major effect on the amount or content of information published on organizational websites and the related information dissemination strategies that they employ.

> We had [self-censored] in the past. We, for example, had almost no content on China on the website … That didn't make much difference [since] blocking in China is something [that] does not seem to depend on how much or what we write on China, but whether the fact that we write generally about human rights.
>
> As an organizational policy, we have not changed our message or softened our stance heavily…I have not seen it once.
>
> We do not craft our information in accordance to censoring rules in countries, our hope is that we can empower activists with tools to reach this information regardless of the fact that it is being or is not being censored.

Non-adopters

The lack of use of either client-side or server-side technologies has mixed effects on information dissemination strategy in the three non-adopting organizations in the sample. While it could be hypothesized that non-adopters would self-censor to prevent censorship since they have no means to counteract it, surprisingly they do not. Further, for the three organizations, the lack of adoption has little to no effect on the overall information strategies when separated from organizational mission. These organizations both maintain a comprehensive organizational policy of openness and consistently post their entire public information flows on organizational websites:

> We put all of our press releases on the website and we operate ourselves sort of on a freedom of information policy … We operate in a kind of way that is as open as possible.
>
> We cannot self-censor ourselves thinking that maybe that information [will lead to censorship] …We are transparent and if information is not nice for the country and they decide something that's their decision.

Despite this lack of a direct effect, one of the organization's subsidiaries (a network member organization) has had a dramatic change in information dissemination strategy regarding their online information flow. In fact, one organization ceased using their public website in 2006 as a means to distribute information directly as a result of domestic Internet censorship. The organization did not adopt circumvention technologies to ensure visibility but instead simply transitioned to other means of information dissemination.

> We have four organizations in Tunisia and none of them have a working website, they just quit with it … if you look at the [organization's] website, you would realize the latest information is from 2006, it's not updated at all, because they know that inside their country and for their members it's not relevant anymore, it's not efficient anymore.

These findings from both adopters and non-adopters suggest that the political sensitivity of information neither influences nor is influenced by circumvention technology use.

Overall, this deductive analysis suggests the organizational characteristics most likely to influence use of circumvention technologies are mission, IT infrastructure, awareness, and IT competency. Technical characteristics influencing use, while appearing to be less influential than organizational characteristics, include effectiveness as well as ease of use and implementation cost, which appear to be related. Finally, as mentioned above, the proposed dual relationship between circumvention technology use and information dissemination strategy was largely refuted.

Inductive analysis findings

Inductive coding reveals findings concerning the role of security, the overall complexity of ICT, and how Internet censorship can have important effects beyond information-related practices.

While this study focuses on the use of technologies to circumvent censorship, informants also discussed security-related technologies and practices critical to their organizational activities. Often times in the process of researching human rights abuses and the transportation of illegal or dangerous information, the safety of human rights organization staff is in jeopardy. In two cases, physical security was discussed in specific detail, but it was also indirectly mentioned by each of the organizations studied as a broader concept. In one instance, an organization had limited the type of information on its public website not to prevent blocking or other forms of censorship, but to ensure the safety of traveling staff members. In the second case, IT staff established information protocols and support for researchers operating in dangerous countries where safety is a primary concern. Here, information is moved quickly from specially trained researchers in the field and security-based hardware/software are used to ensure maximum safety.

> The restrictions that we put on ourselves, in some aspects, are to protect the freedom of movement of our staff going into certain countries … The reason why we would limit what we write on certain countries might be to continue being able to immigrate to that country for trips…
>
> We have high security missions, we classify [researchers a] certain way, we give them different technology … we try to have the information on them as short as possible. Meaning if you are an emergency researcher and you go into a high risk environment, we would give you a device, for example, that if you lose it, no one could even break into it, even if you try … cracks and things like that. On the other hand, we try to have the information out of your hands as soon as possible.

In addition to physical security, the complexity of data transfer and information exchange over the Internet also impact human rights organizations. Two informants specifically described how the fundamental characteristics of the Internet have impacted perceptions of censorship and strategies to mitigation strategies. One informant described how the vastness of the Internet makes it difficult to differentiate systematic communication problems *vs* random interruption. A second informant described state-sponsored censoring tactics.

> The whole Internet is so big and so complex that emails bounce back to us and we have no idea why. … sometimes it'll go through one day and it won't the next day and we don't know why. The very complexity and bulk of the Internet poses certain challenges that are hard to figure out.
>
> There are many people that are surprised at how deep the censorship can go and how complex the system of information exchange in the Internet is. [It can happen] by preventing access at the network level with filtering software and filtering mechanisms, it can be by exerting influence on the host of the website, it can be … by effecting the particular organization's Internet connection from the office.

While in its design this study presumed Internet censorship primarily affected information dissemination strategies, interview data show effects beyond the adoption or non-adoption of censorship circumvention technologies. One informant indirectly described Internet censorship as influencing the location of a regional office and a second detailed the lack of censorship circumvention technology adoption and activity in China as a direct result of censorship there. In fact, since the mission of the organization involves the direct training of partner organizations to use ICT to disseminate local information in countries worldwide, this response to censorship has far reaching implications.

> I think that our mission would not function [in China], so I think that a lot of choosing our partners is based on how much we can help, and we can only help so much when governments and outside forces are censoring the message. Getting the message out is hard enough without those sort of things coming at you, and there are so many organizations looking for our help so we try to focus on those that we can help the most.

Discussion

The above results provide the basis for both a revised model of censorship circumvention technology adoption in human rights organizations and a new broader model of human rights information flows. These models are discussed in the following paragraphs, together with observations on the social context of Internet censorship.

Revised censorship circumvention technology adoption model

Figure 2 depicts a revised organizational adoption model, incorporating changes in technical, organizational and effects variables as well as the dependent variable of circumvention technology adoption. The findings that underlie these changes have several implications for organizational informatics and information systems security research.

The first change is an aggregation of technical characteristics and presentation in a smaller box to reflect their lesser role relative to their organizational counterparts. While users voiced concerns about the technical characteristics, they were infrequently mentioned as reasons not to use the technology. Non-users generally were unaware of or lacked experience with the technologies. Consequently, when considering adoption of complex and immature technologies, technical characteristics are less likely to explain non-adoption.

The second change is the disaggregation of organizational characteristics into 'information and organization,' 'resources,' and 'countries of operation.' The 'information and organization' factors include audience/mission, importance of censorship, and the role of IT. The change from 'mission' to 'audience/mission' is intended to more explicitly depict the role of organizational missions, which define the audiences for circumvention technology use. Similarly, we change 'perception/awareness of censorship' to 'importance of censorship,' putting greater emphasis on the judgment made after awareness is achieved, which has a more direct connection to circumvention technology use. This distinction explains situations where censorship is relatively unimportant to accomplishing a mission or, as will be discussed below, reflects the trade-off to be made in deploying resources to thwart censorship.

Hence, awareness becomes an antecedent to 'importance of censorship.' This finding suggests that IS security adoption research should expand the concept of awareness, integrating subsequent judgments, and expanding beyond awareness of the effects of negative technologies,[5] also to include awareness of the security (or lack thereof) afforded by protective technologies.

Our research shows that systems for censorship detection are lacking, which results in what is denoted in the technical literature as 'the apparition of insecure states' (Debar *et al*., 1999). In addition to a lack of tools for automatic detection, awareness of website blocking may be further hampered by organizational strategies such as outsourcing. In some human rights organizations censorship detection occurs through communication between field personnel and IT staff. Where IT staff are transient or out-sourced, these channels of communication can be disrupted, leaving organizations unaware of blocking. To date, organizational analyses of detection, which largely focus on *intrusion* detection and the IT tools and work associated with these processes (e.g. Goodall *et al*., 2004; Werlinger *et al*., 2008), describe a complicated task within relatively resource-rich IT departments. While these studies shed light on the challenge of communicating detection to the rest of the organization, they should expand the notion of detection to include the informal detection systems that may be more appropriate for human rights organizations.

The third and final information and organization variable is the role of IT. Where the IT office is central within the organization, for example playing a role in strategic planning, the greater the likelihood of circumvention technology use. While the positive relationship between the centrality of IT and adoption is well understood in the general IS adoption literature, it is of special significance here as the centrality of IT is defined in an environment with unique contending forces. Whereas information dissemination, which is strongly associated with IT, plays a central role in many human rights organizations, restrictions on ‘overhead’ – including IT – in the non-profit context tend to limit its importance.

The findings above support the direct relationship between the information and organization variables and circumvention technology adoption; however, there were also frequent references made to the influence of resources. This suggests a moderated relationship wherein the influence of information and organization variables on circumvention technology use may be reduced, strengthened or eliminated altogether, depending on the resources of both the organization and its broader environment.

While the role of resources in IT use, particularly in small and non-profit organizations, is well known (Corder, 2001; Saidel and Cour, 2003; Hackler and Saxton, 2007), our findings provide insight into both their implications for *protective* technology adoption in particular, as well as the relative role of organizational and environmental resources in that process. For example, while all the organizations in our sample employed at least basic IT systems (websites, listservs, email, etc.), in three out of seven no censorship circumvention tools were in use. Also, general resource constraints may affect protective technology adoption in unforeseen ways. Whereas resource and IT-skill-rich organizations benefit in their protective technology adoption from the norms established in social networks of highly skilled users (Dinev and Hu, 2007), human rights organizations may not experience this benefit. Further, given the additional challenges faced by protective *vs* positive technologies, resource limitations may play an even greater role in explaining their adoption.

In addition to organizational resources, we also include countries of operation, in particular their censorship activity/effectiveness, as moderating variables. While ‘audience/mission’ can shape an organization’s broad geographical focus of operations, the scope of Internet and information censorship activity and enforcement (encompassing threats to physical security) varies across countries. The extent to which a country engages in visible censorship and/or enforces penalties on violators may interact with organizational traits to shape the need (or lack thereof) for the adoption of censorship circumvention technologies and subsequent behavior. As an example, if ‘information and organization’ characteristics suggest censorship circumvention technology adoption is beneficial to organizational operations yet censorship and enforcement is high, an organization may select non-adoption in particular countries and simply pursue alternative strategies as mentioned above.

Lastly, the revised model specifies effects of adoption or non-adoption, including a broader range of information dissemination strategies. The findings suggest circumvention technology non-use may affect information dissemination in several ways, including use of other media, exiting the web altogether or in very limited cases self-censorship, while the use of circumvention technology typically supports already ongoing dissemination strategies or increased availability of information (i.e. via mirroring). In some cases, non-adoption may precede an organization’s decision about where to operate, though more specific future research should examine the extent to which human rights organizations not making use of circumvention technologies avoid operating in censoring countries.

The final change to our original model is seen in the disaggregation of circumvention technology adoption into server-side and user-side, a reflection of their configurability (Sawyer and Rosenbaum, 2000). Our research suggests user-side circumvention tools have lower barriers to adoption, in terms of resources and IT competency, than server-side technologies. Also, an organization’s mission/audience is likely to play a more significant role in server-side adoption as compared with user-side. Hence, as predicted by organizational informatics, the effects of organizational characteristics vary across levels of the ICT architecture.

Human rights information flows

Additional findings are depicted in a model (Figure 3), situating the human rights organization in its broader information flows and highlighting interesting dualities and effects of these flows on physical security.

In this expanded model the human rights organization is characterized by two key elements affecting information flows, namely the information dissemination strategy and circumvention technology use. These two factors define and in turn are defined by the audience and this duality impacts the extent to which information is received by that audience, typically in a broadcast mode. The model further delineates the role of field staff/researchers and victims of human rights abuses, who similar to the audience are involved in a duality that influences information flows.

This model highlights information security as critical to safeguarding physical security. To date, concerns about physical security in information security are largely related to physical access. Corporate IT professionals have called for greater attention to physical security, advocating for the integration of corporate functions of physical and information security to better enhance both (e.g. Radcliff, 1998; Myler and Broadbent, 2006). However, here the issue is slightly different, with the threat to physical security arising from possession of politically sensitive information. While this topic has likely received significant attention in classified research on intelligence gathering and the protection of intelligence agents, academic research on these issues as experienced by human rights and other advocacy communities has yet to be carried out. By further exploring topics such as the conditions of use of IT security devices by human rights researchers, ICT researchers may develop a more nuanced understanding of open access and information flows, both when desirable, as in the case of human rights abuses, as well as when undesirable (e.g. black markets for nuclear weapons).

Additional observations on internet censorship

Human rights information flows are embedded in the broader context of censoring and circumvention, a dynamic cat-and-mouse game in which technologies and strategies on both sides are constantly evolving. Additional observations by our informants suggest some censoring nations encounter hurdles in their attempts to control information flows, while others are more nimble, implementing more nuanced strategies. One informant detailed the case of a country that unsuccessfully employed a brute force approach, namely disconnecting the nation’s network from

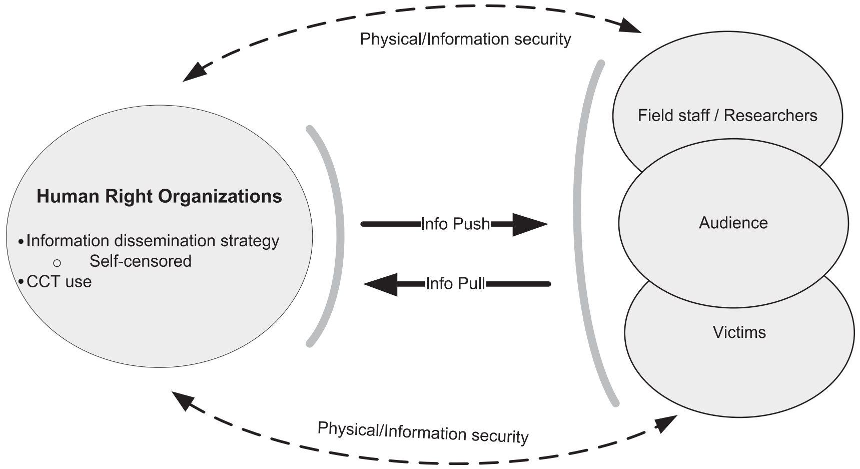
Physical/Information security
Field staff / Researchers
Human Right Organizations
• Information dissemination strategy
○ Self-censored
• CCT use
Info Push
Info Pull
Audience
Victims
Physical/Information security

Figure 3 The flow of human rights information.

the global Internet, underestimating the degree to which its government infrastructure and government officials were dependent on the Internet.

> When we sent our researcher he told me [that the government] shut down the Internet access for the whole country. Then they couldn't do things themselves and the minute they put it back people were able to evade and he was able to talk to us.

Conversely, other informants described more nuanced strategies employed to influence elections.

> During the elections in Belarus, it can be affecting the national gateway to … slow it down for a particular IP range or IP address … [of] websites that are of particular importance … When targeted censorship occurs in a response to current events or in regards to a particular group of people or particular organization, that is when it is most effective.

Increasing sophistication of governments is likely to be met with similar actions on the part of information seekers. However, as observed by one informant, access to human rights information may not be the direct driver of greater circumvention technology use.

> It's not the politics side, it's the Facebook and the social networking [sites] and those people [who] want to see their American friend and European friend … A lot of countries [are] preventing those sites and a lot of people want to see it and they do use projects like the Tor software to evade it … Once you know how to do it for the Facebook, visiting [our website] or any other site is simple.

Summary and implications of findings

The findings of this research, reflected in the two models and additional observations above, have implications for academics as well as practitioners.

The implications for IS security adoption research stem in part from the unique nature of censorship and circumvention technologies. As security technologies, they seek to avert restrictions on flows or enhance anonymity rather than prevent access or defeat malicious code. Therefore, they can be seen as proactive protective technologies as opposed to reactive, particularly as censorship can be difficult to detect. Hence, this research suggests awareness of the benefits and limitations of protective technologies will affect adoption and that itself awareness may be hampered by underdeveloped detection systems. Finally, the findings suggest resource constraints may more strongly influence adoption of protective, as compared with productivity-enhancing positive, technologies.

The findings also provide further support for two key dimensions of the organizational informatics approach. Having both server- and client-side components, circumvention technologies are configurable, experiencing different effects of organizational characteristics across these two levels. Also, the duality of influence between the organization and ICTs is observed in the role the audience plays in defining the initial impetus for server-side circumvention technology use, but subsequently diminishes that need as client-side use becomes more prevalent.

This dynamic raises interesting questions for future research with implications for both information systems security and organizational informatics. For example, while organizations' adoptions of circumvention technologies were hampered by a lack of IT skills and resources, there also appeared to be a sense of powerlessness or resignation to the government actions. Future research might seek to uncover the extent to which this is related to issues of detection, or whether it is based on an expectation of a technological trajectory, such as the one discussed above, whereby client-side use becomes so ubiquitous as to render server-side efforts unnecessary.

This research suggests the following for human rights organizations and their supporters. First, human rights organizations should take into account the potential role communication between field and IT staff may play in detecting censorship when making decisions about IT outsourcing. Currently, technical means for detecting censorship are fairly underdeveloped and first-hand reports by those in the field are an important mechanism for detecting censorship. Second, for those organizations promoting circumvention technology use by their audience, it may be beneficial to assess critically various audience segments' capacity to use these tools. Systematic analysis will help the organization understand who is and is not receiving their message. Finally, organizations seeking to support human rights organizations might supply simple circumvention technologies packaged together, similar to the concept of 'non-profit in a box,' in which all the necessary software is put together in one easy-to-use bundle, including tips for mirroring sites to minimize chances of being blocked, technologies (yet to be developed) to automatically detect and mitigate censorship, and a 'PC on a stick' that can be easily deployed to field staff and the audience.

Conclusion

As governments increasingly restrict information flows, particularly of political information, a variety of organizations, including media and human rights organizations, are affected. Given the likelihood of being targeted, human rights organizations' responses to censorship may provide insight into the impact of this phenomenon.

This exploratory research, guided by an organizational informatics framework, examined a particular response – the use of censorship circumvention technologies. The study examined the organizational and technical characteristics influencing (non) adoption and use, and their subsequent effects on organizational strategies. Despite having information dissemination as a primary mission and recognizing their websites are likely being blocked, this research finds, contrary to our expectations, use of these technologies is not widespread. Only two of the seven organizations employed server-side technologies to enhance access to their websites, while a little over half employed client-side technologies. Factors explaining these findings include the audience and importance of Internet censorship to the organization, as well as resource limitations. The study results in two models, which can serve as the basis for future research, one specifying variables to explain circumvention technology adoption and use and a second that depicts the factors influencing human rights organizations' information flows.

As an indicator of the impact of censorship, this research finds organizations are struggling to systematically detect and thwart website blocking. In one case the censorship has led an organization to abandon the web altogether and in another censorship influenced an organization's countries of operation. Given the limited resources of human rights organizations, client-side circumvention technologies appear to have lower barriers to adoption, providing what is likely a more effective means of circumvention.

As an exploratory study there are many limitations. First, human rights organizations are a heterogeneous group and our sample does not allow us to assess the generalizability of our findings even within this narrow domain. Second, claims such as those concerning the significance of IT to the organization or resource limitations, need to be substantiated by additional interviews within each organization. Third, our conceptualization of censorship circumvention technologies may be too broad. Further delineation of the factors influencing adoption of different types of circumvention technologies may be helpful to information security research.

Despite these limitations, the research has implications for IS security models and the organizational informatics approach as well as for practitioners. The implications for academic research arise from the unique nature of censorship and circumvention technologies as well as the information processing orientation of human rights organizations, in which the audience influences information systems adoption and use. Insights for practice include recommendations both for human rights organizations for detecting censorship and understanding audience capabilities to use circumvention technologies, as well as the technologies they need which might be supplied by their supporters.

Notes

[1] For example, Callanan *et al*. (2011), of Freedom House, analyze various censorship circumvention tools and provide a comparative review of those utilized in Azerbaijan, Burma, China, and Iran. Guides include: 'Leaping Over the Firewall: A review of censorship circumvention tools' (Freedom House), 'Handbook for Bloggers and Cyber Dissidents' (Reporters Without Borders), the 'Everyone's Guide to By-Passing Internet Censorship' (CitizenLab, University of Toronto), and the 'Security in-a-Box' toolkit (Tactical Technology Collective and Front Line).

[2] Organizations originally selected were those that had a name that included (1) keywords like torture, death, justice, accountability, action, and genocide that suggest an actionable and controversial organizational mission likely to incite censorship, (2) geographic descriptors like Arab, Albanian, East Timor, and Asian that suggest operation in countries that either have a history of controversial human rights activities or Internet/other media censorship, or (3) words like freedom, expression, journalists, protection, witness, advocates, and cyber rights that suggested an organizational mission involving activities directly involving freedom of speech and censorship.

[3] As shown in Table A1, interview length ranged from 13 min to over 85 min, with an average interview length of approximately 30 min. Data from interviews were supplemented with contextual information drawn from organizational websites. Some interviews included multiple informants at the same organization. Interviews followed a conversational, semi-structured format with at least one of the authors conducting the interview via standard telephone or VOIP (Skype). Table A2 lists the full set of questions utilized in the interviews, which include overlapping question modules that correspond directly to the specifications of the interaction model and research questions presented above. Some variation in question wording and order was utilized to maintain a conversational tone. In most cases, not all questions were asked, but every effort was made to cover questions across all modules within the time constraints of each informant.

[4] Separate tables foster the required anonymity for informants.

[5] For example, Dinev and Hu (2007) consider only awareness of the potential effects of spyware and the extent which users are aware of whether or not their computers are infected with spyware.

References

Axelrod, R. and Cohen, M.D. (2000). *Harnessing Complexity: Organizational implications of a scientific frontier*, New York: Free Press.

Brophy, P. and Halpin, E. (1999). Through the Net to Freedom: Information, the internet and human rights, *Journal of Information Science* **25**(5): 351–364.

Burt, E. and Taylor, J. (2003). New Technologies, Embedded Value and Strategic Change: Evidence from the U.K. voluntary sector, *Nonprofit and Voluntary Sector Quarterly* **32**(1): 115–127.

Carayannis, E.G. and Turner, E. (2006). Innovation Diffusion and Technology Acceptance: The case of PKI technology, *Technovation* **26**(7): 847–855.

Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A. and Guerra, R. (2011). Leaping Over the Firewall: A review of censorship circumvention tools, [WWW document] http://freedomhouse.org/uploads/special_report/97.pdf].

Corder, K. (2001). Acquiring New Technology: Comparing nonprofit and public sector agencies, *Administration & Society* **33**(2): 194.

Q7 **Debar, H., Dacier, M. and Wespi, A.** (1999). Towards a Taxonomy of Intrusion-Detection Systems, *Computer Networks* **31**: 805–822.

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (eds.) (2008). *Access Denied: The practice and policy of global internet filtering*, Cambridge: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (eds.) (2010). *Access Controlled: The shaping of power, rights and rules in cyberspace*, Cambridge: MIT Press.

Dhillon, G. and Torkzadeh, G. (2006). Value-Focused Assessment of Information System Security in Organizations, *Information Systems Journal* **16**(1): 293–314.

Dinev, T. and Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies, *Journal of the Association for Information Systems* **8**(7): 386–408.

Q8 **Dingledine, R. and Mathewson, N.** (2006). Anonymity Loves Company: Usability and the network effect, in Proceedings of the 5th Workshop on the Economics of Information Security (WEIS).

Q9 **Fabian, B., Goertz, F., Kunz, S., Muller, S. and Nitzsche, M.** (2010). Privately Waiting - A usability analysis of the tor anonymity network, in Proceedings of the 16th Americas Conference on Information Systems (AMCIS) (Lima, Peru, 12-15 August 2010).

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2004). I Know My network: Collaboration and expertise in intrusion detection, *CHI Letters* **6**(3): 342–345.

Hackler, D. and Saxton, G.D. (2007). The Strategic Use of Information Technology by Nonprofit Organizations: Increasing capacity and untapped potential, *Public Administration Review* **3**(67): 474–487.

Q10 **Hernan, S.** (2000). Security Often Sacrificed for Convenience, *CrossTalk: The Journal of Defense Software Engineering*, October.

Hopgood, S. (2006). *Keepers of the Flame: Understanding Amnesty International*, Ithaca, NY: Cornell University Press.

Kling, R. (1993). Organizational Analysis in Computer Science, *The Information Society* **9**(2): 71–87.

Kling, R. (1999). What is Social Informatics and Why Does it Matter, *DLIB Magazine* **5**(1), [WWW document] http://www.dlib.org/dlib/january99/kling/01kling.html.

Q11 **Kling, R.** (2000). Learning about Information Technologies and Social Change: The contribution of social informatics, *The Information Society* **16**(3).

Kling, R. (2001). Social Informatics, *Encyclopedia of LIS* [WWW document] http://rkcsi.indiana.edu/archive/SI/si2001.html.

Lamb, R. and Kling, R. (2003). Reconceptualizing Users as Social Actors in Information Systems Research, *MIS Quarterly* **27**(2): 197–235.

Maitland, C.F. and Tapia, A. (2007). Coordinated ICTs for Effective Use in Humanitarian Assistance, *The Journal of Information Technology in Social Change* **1**(1): 128–141.

Markus, M.L. and Robey, D. (1988). Information Technology and Organizational Change: Causal structure in theory and research, *Management Science* **34**(5): 583–598.

Mitleton-Kelly, E. and Land, F. (2004). Complexity and Information Systems, in C. Argyris and Starbuck (eds.) *Blackwell Encyclopedia of Management*, Oxford, UK: Blackwell Publishing Ltd.

Myler, E. and Broadbent, G. (2006). ISO 17799: Standard for security, *Information Management Journal* **40**(6): 43–52.

National Research Council (2010). *Toward Better Usability, Privacy and Security of Information Technology*, Washington DC: National Academies Press, p. 207.

Orlikowski, W.J. and Iacono, C.S. (2001). Research Commentary: Desperately seeking 'IT' in IT research - A call to theorizing the IT artifact, *Information Systems Research* **12**(2): 121–134.

Orlikowski, W.J. and Robey, D. (1991). Information Technology and the Structuring of Organizations, *Information Systems Research* **2**(2): 143–169.

Orlikowski, W.J. (1993). Learning from NOTES: Organizational issues in groupware implementation, *The Information Society Journal* **9**: 237–250.

Radcliff, D. (1998). Don't Forget the Guard, *Computerworld* **32**(25): 66.

Rubenstein, L.S. (2004). How International Human Rights Organizations can Advance Economic Social, and Cultural Rights: A response to Kenneth Roth, *Human Rights Quarterly* **26**(4): 845–865.

Saidel, J.R. and Cour, S. (2003). Information Technology and the Voluntary Sector Workplace, *Nonprofit and Voluntary Sector Quarterly* **32**(1): 5–24.

Sawyer, S. and Rosenbaum, H. (2000). Social Informatics in the Information Sciences: Current activities and emerging directions, *Informing Science* **3**(2): 89–96.

Scott, W.R. (1995). *Institutions and Organizations*, Thousand Oaks, CA: Sage Publications.

Straub, D.W. and Nance, W.D. (1988). Uncovering and Disciplining Computer Abuse: Organizational responses and options, *Information Age* **10**(3): 151–156.

Straub, D.W. and Welke, R.J. (1998). Coping with Systems Risk: Security planning models for management decision making, *MIS Quarterly* **22**(4): 441–469.

Suparamaniam, N. and Dekker, S. (2003). Paradoxes of Power: The separation of knowledge and authority in international disaster relief work, *Disaster Prevention and Management* **12**(4): 312–318.

Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P. and Beznosov, K. (2008). The Challenges of Using an Intrusion Detection System: Is it worth the effort?, in Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08), pp. 107-118.

Zafar, H. and Clark, J.G. (2009). Current State of Information Security Research in IS, *Communications of the Association for Information Systems* **24**(1): 572–596.

Zittrain, J. and Edelman, B. (2003). Internet Filtering in China, *IEEE Internet Computing* **7**(2): 70–77.

About the authors

Carleen Maitland is an associate professor in Penn State University's College of Information Sciences and Technology. Her research examines the international and inter-organizational context of information technology use. Recent studies have analyzed coordination of information technology and information management across humanitarian relief organizations, including the United Nations Office of Coordination for Humanitarian Affairs. She also studies international telecommunications policy coordination. In 2010-2012, Dr. Maitland served as a Program Manager in the US National Science Foundation′s Office of International Science and Engineering.

H.F. Thomas III (Trey) is a doctoral student in the Department of Government at the University of Texas at Austin. Trey holds B.Phil. and M.A. degrees from Penn State University and an M.A. from UT Austin. His research interests include agenda-setting, public policy processes, lobbying and interest groups. Trey' current research utilizes network analysis and agent-based simulation techniques to understand how contagion among policymakers shapes macro-level patterns in government activity.

Louis-Marie Ngamassi Tchouakeu received his Ph.D. in 2011 from the College of Information Sciences and Technology at Penn State University. He is currently an Assistant Professor of Management Information Systems at Prairie View A&M University, College of Business. His research focuses on information and communication technology (ICT) use for inter-organizational coordination and social networks among humanitarian organizations.

Appendix

Table A1 Interview date and length

Interview date	*Length of the interview*
3/21/2008	1:15:44
3/28/2008	0:42:25
8/4/2008	0:15:48
8/6/2008	0:14:10
8/6/2008	0:13:21
9/26/2008	0:30:01
2/20/2009	0:28:51
4/9/2009	0:27:16

Note: Average interview length is approximately 30 min. Some interviews included multiple informants.

Table A2 Semi-structured interview questions

General

1. Could you briefly explain your position and role in your organization?
2. Could you shortly describe your background/career in the Human Rights field?
3. How long have you been a part of your organization?

Organizational context

1. What is the main purpose of your Human Rights (HR) organization? (lobbying for policy change, providing services, monitoring conditions, etc.)?
2. What are the main activities of your HR organization?
3. Which other organizations do you find yourself most similar to and how do you feel you are different from them?
4. What type of organization (membership, etc)?

Structure/geography

1. In what countries does your organization undertake human rights activities?
2. Where are the headquarters located?
3. How many field offices does your organization operate and where are they located?
4. Where is your IT infrastructure located?
   a. Are they distributed among satellite offices or centralized at the headquarters?
5. What is the decision-making structure for IT-related issues?

Technology competency

1. How many full-time IT staff does your organization maintain?

2.Do satellite offices maintain full-time IT staff?

3. Do full-time IT staff have other non-IT duties?
4. Does your organization maintain part-time staff or interns for IT-related tasks?
5. Where in your organizational structure does your IT person fall and who do they report to?
6. Could your rate the competency of your IT staff on a scale of 1-10 (1 being the least competent and 10 being extremely competent and knowledgeable)?
7. How much emphasis does your organization place on information technology?
   a. What about adopting new technology?

Information flows/information dissemination strategy

1. Does your organization have a specific information dissemination strategy (IDS)?
2. How does your organization disseminate information?
   a. What role does the dissemination of information play in your organization?
3. *Before interview, look at website* I notice on your website that you have _________, is this typical of the information you post on your website?
   a. What is the intended audience (people living in countries where you are active, journalists, US citizens, decision-makers…?)
4. Does your organization limit the type and controversial nature of the information published on your website or in communications with offices in other countries?
5. How are decisions made regarding what information is made public and how?
6. How centralized is your information dissemination strategy? (For example, are decisions about the content and type information distributed publicly made at satellite offices or at headquarters)?
7. Does each satellite office maintain its own website, or part of the central website on their own?

Perception of threat/experience with censorship

1. Are you aware of issues surrounding Internet censorship?

a. If yes, do you perceive Internet censorship (the blocking of your organizational website, communications or news articles about your activities) as a problem or threat to the goals of your organization?

i. If no, could you discuss the priorities of your organization related to the IT infrastructure in the context of your organizational mission?

2. How likely do you think it is that your official Internet-based communications will be censored in the future in the countries you are active in?
3. To your knowledge, has your organization been the subject of Internet censorship?
   a. If yes, how many instances of censorship?
   b. Could you please describe the most significant instances and the context in which they were discovered?
   c. Did you take any preventative/reactionary measures against the censorship? (if participant describes CCT use, skip to CCT adoption questions)
   d. Does your org have the tools to recognize/detect if your website was censored or blocked in another country?

Table A2 Continued

4. Has your organization taken any steps to reduce the likelihood of being censored, excluding any technical solutions?
5. Scenario – if your organization found out about a human rights violation in a country that isn't being reported in the mass media, how likely would your organization be to post such information in Internet-based communications?

CCT adoption

1. Has your organization implemented CCT (which includes counter-filtering in anyway)?
    a. If so, which technologies and for what specific purposes?
    b. Where is this technology used – at headquarters or in satellite offices?
    c. Use related to centralized control?

CCT characteristics

1. If adopted: Let's talk about how you found the technology, what features you require, etc.
2. What characteristics of the CCT you use that make them attractive?
3. Could you talk about the ease of use, effective, features, cost?
4. What characteristics of the CCT you use would you change to make it better?
5. If not, are there any characteristics of CCTs that make them unattractive?
6. Would you use them if they were easier to implement in your organization?
    a. More effective?
    b. Had more features?
    c. Were less costly?
    d. Required less technological competency?

S.I. related effects

1. Has your organization's IT infrastructure or information strategies changed as a result of the threat of Internet censorship?
    a. If so, could explain, in detail, these effects?
2. Have there been any changes (structure, processes, activity) in your organization as a result of the threat of Internet censorship?
3. Is your organization involved in any coalition-based efforts to learn about protecting your organization against Internet Censorship?
    a. If not, do you think your organization would get involved with such a coalition if it existed?

Other contacts

1. Are you aware of other international human rights organizations that have been the targets of censorship or have a knowledge of the threat of Internet censorship?
    a. If so, could you provide the names (and any contact information) of up to five organizations?
2. If your organization was the target of censorship, would you contact any other organizations/individuals for help?
    a. If so, could you provide the names (and any contact information) of up to five organizations?
3. Could you provide (up to five) the names and contact information for co-workers or others who may be interested in providing us with their experience regarding Internet censorship and its effect on international human rights organizations?

Note: Nearly all questions in the conducted interviews are shown above, though some follow-up questions and slight deviations were utilized to maintain a conversational tone with respondents. Not all questions above were asked given time constraints, but every effort was made to address the various major topics of each section.

Table A3 Deductive analytic coding scheme

RQ#1 – How does Internet censorship impact human rights organizations?
RQ#2 –To what extent do human rights organizations make use of CCTs?
RQ#3 –How does this (lack of) use influence organizational processes and strategies?
Model Component – Type of use
Model Component – Ease of use
Model Component – Effectiveness
Model Component – Implementation cost
Model Component –Structure/geography
Model Component – IT competency of staff
Model Component – IT infrastructure/adopting new technology/emphasis on both
Model Component – Perception/awareness of Internet censorship
Model Component – Mission/likelihood of being censored
Model Component –Countries of operation
Model Component – CCT adoption
Model Component – Degree of centralization

Table A4 Inductive analytic coding scheme

Inductive Coding – Decision-making process
Inductive Coding – Information dissemination strategy
Inductive Coding –Target population/audience?
Inductive Coding – Censorship *vs* other Internet access problems
Inductive Coding – Use of IT consultants
Inductive Coding – Role of IT in the organization
Inductive Coding – Adopting new technology
Inductive Coding – Collecting information on/research of technology
Inductive Coding – General effects of lack of IT skills on human rights information flows
Inductive Coding – Adopting new technology

Note: Interviews with HRO staff members were coded by the authors according to the above analytical coding schemes (topic-based).