Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

A STRUCTURED STAKEHOLDER SELF-IDENTIFICATION APPROACH FOR THE DEPLOYMENT OF PUBLIC INFORMATION SYSTEMS: THE CASE OF SURVEILLANCE TECHNOLOGY IN THE CITY OF PITTSBURGH

ENRIQUE MU
CARLOW UNIVERISTY
emu@carlow.edu

HOWARD A. STERN
CARLOW UNIVERSITY
hastern@carlow.edu

ABSTRACT

The deployment of information technology (IT) in the public sector is particularly difficult due to the large number of stakeholders and the challenges in identifying them. This is particularly true in the case of innovative IT technologies. To date, normative methods of stakeholder identification have not been developed. To solve this impasse, an approach to the identification of stakeholders in the deployment of public information systems – called the *structured stakeholder self-identification process* – is proposed here. This approach, based on the theory and practice of public participation and stakeholder identification theory, is discussed and illustrated with a case study: the deployment of surveillance technology in the city of Pittsburgh.

Keywords: Structured stakeholder self-identification, stakeholder self-identification, stakeholder management, public information systems, IT public participation, IT public sector, public IT innovation, public surveillance systems

INTRODUCTION

Since the milestone work of Freeman [10], stakeholder management has been part of the toolkit of strategic management, particularly in the public sector, where there is a great demand for openness and accountability [31]. In effect, one key distinction between public and private sector management is that the former requires a great deal of transparency and interaction with a large number of stakeholders, many of whom are quite vocal and organized, and whose actions will play a decisive role in the adoption and public acceptance of proposed actions [5]. The deployment of information technology in the public sector is particularly difficult due to, among other things, the presence of multiple stakeholders with competing goals [31]. Therefore, identifying stakeholders and satisfying their needs according to their importance or salience is vital to the success of information systems in the public arena. Typically, stakeholder identification is left either to the agency staff, ad-hoc committees, or the discretionary will of stakeholders to identify themselves [40, 6]. There are, however, few normative approaches to stakeholder identification that staff and committees can use to ensure no stakeholders are left out [25]. Also, voluntary appearance of stakeholders may occur too late in the

process (for example, when stakeholders identify themselves as such to protest the system deployment). Furthermore, the task of identifying stakeholders becomes more problematic when deploying an Information Technology (IT) innovation. This is because the more complex and interrelated the IT, the more difficult it will be to anticipate its interactions , who will be affected, and how they will be affected by the IT deployment [29]. In other words, the more innovative the IT, the more difficult it is to anticipate salient stakeholders. To deal with this problem, this research proposes a novel approach called "structured stakeholder self-identification" to identify salient stakeholders when deploying a public information system. This approach builds upon both stakeholder management and public participation theory and practice, and is aimed at systematically eliciting stakeholder self-identification. Furthermore, the proposed approach is illustrated with a case study in the City of Pittsburgh. The rest of this paper is organized as follows: first, stakeholder management will be reviewed; second, the issues associated with the deployment of public IT will be discussed; third, a discussion of how the City of Pittsburgh solved the problem of stakeholder identification using the proposed "structured stakeholder self-identification" process[1] when deploying a public surveillance system will be described and fourth, the conclusions and lessons learned from this case study will be discussed.

STAKEHOLDER MANAGEMENT

Since its inception, stakeholder management theory has been widely used in both the private sector and public administration [11]. A stakeholder in an organization denotes "any group or individual who can affect the achievement or is affected by the achievement of the organization's objectives" [36, 10]. This broad definition is used here because it is the most inclusive of a wide variety of potential stakeholders [25]. Stakeholder management has a long tradition in the administration of environmental resources [13] and public policy at large [4, 5]. More recently, stakeholder management theory has become particularly relevant for social responsibility and organizational performance [17, 11]. Still, one unresolved issue with stakeholder management theory is that a systematic normative approach to identifying stakeholders has not been developed [25, 38]. Most studies of stakeholder identification use rather descriptive approaches, such as distinguishing between the "involved" and the "affected" [38] or classifying stakeholders in terms of power, legitimacy, and urgency [25].

Mitchell et al. [25] is probably the most widely used and cited of the different descriptive frameworks developed. Mitchell developed a typology of stakeholders based on a combination of three attributes: (1) power – an individual or group that can directly impact the project, (2) legitimacy – the perception that an individual or group has the ability or clout to influence a project, (3) urgency – the immediate need to deal with an individual or group's concerns. Based on a combination of these three attributes, stakeholders can be classified in seven types: dormant, discretionary, demanding, dominant, dangerous, dependent, and definitive. This is not the place to discuss this well-known framework in detail (see Appendix A)[2], except to mention the importance of identifying, in particular, the "definitive stakeholders"; that is, those who possess all three attributes – power, legitimacy, and urgency. Leaving any definitive stakeholder out may have serious consequences for the organization since these are the stakeholders to whom managers must pay particular attention [25]. This typology of stakeholders is important because satisfying the needs (sometimes contradictory) of all possible stakeholders is not realistically possible; however, any public IT deployment should carefully consider, at least, the needs of the "definitive" stakeholders.

Unfortunately, as Mitchell et al. [25] clearly indicate, their framework is descriptive rather than normative, so the question of who belongs on a stakeholder list is still present. In fact, a quick review of the literature shows that all stakeholder identification analyses assume that it is possible to know a priori who the stakeholders will be. That is, it is assumed that somehow managers and/or a group of expert advisors will eventually find out, through hard thinking, who the organization's stakeholders are [1, 30]. Although the literature on the management of natural resources has suggested the need to get public participation for some time [18, 6], a review of the public administration literature shows that this approach is not widely used.

Probably the best illustration of the above assumption is found in "Strategic Planning for Public and Non-Profit Organizations" by Bryson [5], one of the most popular textbooks in the field used to train the new generation of public administrators. This textbook discusses fourteen different approaches to the task of identifying stakeholders. Upon close examination, all fourteen approaches share the fundamental assumption

[1] The term "structured stakeholder self-identification" has been created to better summarize the approach proposed in this paper.

[2] For the benefit of the readers unfamiliar with this typology, a brief summary is provided in the appendix.

that, through brainstorming and related processes, a suitable committee will be able to identify all possible stakeholders a priori. To minimize the possibility of leaving out a salient stakeholder, many practitioners emphasize the great importance of the stakeholder identification committee and its composition [5]. The implicit rationale is that a well-constituted committee will eventually succeed in identifying all potential stakeholders.

The problem of improper stakeholder identification is even more important in the case of deployment of IT innovations in the public sector. The central argument made in this paper is that no matter how carefully the committee is chosen, the nature of an IT innovation makes the a priori identification of salient stakeholders very difficult, if not impossible.

Still, stakeholder identification is key for strategic management, particularly in the public sector where openness and transparency are required [5]. Therefore, as more novel innovations are deployed in the public sector, there is a more pressing need to identify the relevant stakeholders, in particular, the salient ones. Willeke [40] and Creighton [6] suggested stakeholder self-identification (to volunteer or to express opposition) as a third way (in addition to the use of agency staff and committees) to identify stakeholders. However, stakeholder identification management, in particular getting stakeholders to self-identify, has been addressed mainly in the domain of natural resources management. There is a serious gap in the IT management literature in the public sector about how to do this early on in a systematic way. How will potential stakeholders learn about the project and step forward to self-identify as a stakeholder? As Heathcote [18] points out, "self-identification" may be perceived as more in keeping with a spirit of openness and transparency than identification by an external (possibly biased) group" but, she goes on to say "self-identification may be more complex than Willeke suggests; however, because of the difficulty in providing adequate notice to the public that opportunities for involvement exist" [40, p. 111]. In order to address the need to create community awareness leading to systematic and timely stakeholder self-identification, this research borrows from stakeholder management and public participation theory and practice to propose the use of the "structured stakeholder self-identification" approach, which facilitates the identification of potential stakeholders, in the deployment of public IT innovations. This approach is described within the context of a case: the deployment of a new public information system – a surveillance system in the City of Pittsburgh.

ISSUES ASSOCIATED WITH THE DEPLOYMENT OF PUBLIC INFORMATION TECHNOLOGY

Any information technology used in the public sector constitutes a public management information system according to the seminal discussion of the topic given by Bozeman and Bretschneider [3]. There are important differences between public and private management information systems [33] such as the ones summarized by the Center for Technology in Government and Rocheleau [31, pp. 2]: a) less inclination to invest in risky technologies; b) divided authority over IT decisions due to legal, bureaucratic, and political constraints which makes it harder to manage the IT projects; c) presence of multiple stakeholders with conflicting goals; d) one-year budgets, which make it more difficult to plan long term; e) highly regulated procurement through the bidding of competitive contracts and Requests for Proposals (RFPs); and f) many other factors, such as inter-agency linkages that make it difficult to undertake changes without affecting other agencies.

Interestingly enough, and based on our review of the literature, stakeholder management in the deployment of public information systems and IS in general has focused mainly on the proper collection of user requirements for system development rather than in the public response to the IS [19]. As an example, in a 1995 survey to public CIOs about the pressing issues in their field, none of them indicated stakeholder identification and management as an important issue while getting proper information requirements ranked number 12 in the list of 45 issues [34]. One reason for this lack of concern for stakeholder management (outside getting users' requirements) may be that, differently from environmental projects affecting natural resources, public IS has not been traditionally perceived as a politically charged project requiring broad public acceptance for success. Still, there is evidence that factors such as mistrust, forming of opposition coalitions, and other similar political factors may lead organizational stakeholders to create obstacles to the IS implementation [28]. These factors may also lead the general public to oppose a specific IS project, sometimes to the point of closing it, as was the case with the proposed government's public policy electronic market labeled as 'terrorism's futures market' by its opponents [20].

In conclusion, multiplicity of actors or stakeholders with conflicting goals is one of the key characteristics of public information systems. There is evidence that stakeholders' opposition may lead IS private and public deployments to fail; still, stakeholders

identification in IS has been mainly limited to requirements engineering. Furthermore, in the case of IT innovations, it is hard to identify all possible relevant and diverse stakeholders. The more complex the IT innovation, the harder it will be to anticipate unexpected effects, unintended stakeholders, and their interrelations [29]. This research will propose a process, borrowing from techniques widely used in natural resource management, for stakeholder identification in public information systems, within the context of the deployment of a surveillance system in the City of Pittsburgh.

Surveillance refers to efforts to gather information about people from a distance without entering into private spaces [32]. A modern surveillance system uses sophisticated video analytics that can trigger an alert at the sound of a gun, employ facial recognition software that can be cross-referenced with national databases, and many other complex applications. In other words, a surveillance system is a much more complex technology than just a camera capturing images and has evolved into the field of video analytics [2]. Because of this, a public surveillance system can be considered as a public management information system deployed by the government (either local or federal) and aimed at collecting, processing, and storing information about people in public spaces [32].

Several local governments (including Baltimore, Buffalo, Chicago, and Phoenix) have already deployed public surveillance systems to deter criminal activity and prevent terrorism in key areas of the city [2, 22]. Still, this deployment constitutes a recent IT innovation in many cities, which has generated concerns among different people and organizations [32] and has led, in most cases, to the elaboration of thorough privacy guidelines for its use [8, pp. 10]. These privacy and usage guidelines, key to the successful deployment of surveillance systems, must be developed in collaboration with the different system stakeholders to ensure that their needs are met. Unfortunately, this is not an easy task due to the multiplicity of stakeholders and the lack of clarity about whom the stakeholders are and which of them (in other words, who are the most salient or important) should participate in the elaboration of these policies (e.g. the "definitive" stakeholders in Mitchell et al. [25] terminology). So, identifying the salient stakeholders becomes a key factor in the development and elaboration of a policy framework prior to the deployment of a public surveillance system. Also, having the acquiescence and backing of salient stakeholders will increase the likelihood of public support for the deployment of the surveillance system and its successful adoption. For this purpose, the rest of this paper will discuss the City of Pittsburgh's use of a newly developed "structured stakeholder self-identification" approach to identify the system stakeholders.

THE CASE OF SURVEILLANCE TECHNOLOGY IN THE CITY OF PITTSBURGH USING THE STRUCTURED STAKEHOLDER SELF-IDENTIFICATION PROCESS

One might think that a sophisticated surveillance system that can link hundreds of cameras throughout the city, possess night vision with high resolution, notify authorities at the sound of a gunshot, identify a person by scanning her retina, notice suspicious activities, or compare images from a national database of suspected terrorists would still belong to the realm of action movies and spy thrillers. However, such technology exists and has been tested many times across the country (Figure 1). Furthermore, one might expect the community to unanimously embrace the deployment of such a technology, but the reality is quite different. Unfortunately, the political, bureaucratic and social issues raised by a sophisticated camera system can cause such a project to experience significant delays or even to be scrapped altogether. This case study illustrates the many stakeholders in a government-sponsored surveillance system, and describes the "structured stakeholder self-identification" approach developed with the purpose of identifying the key stakeholders.

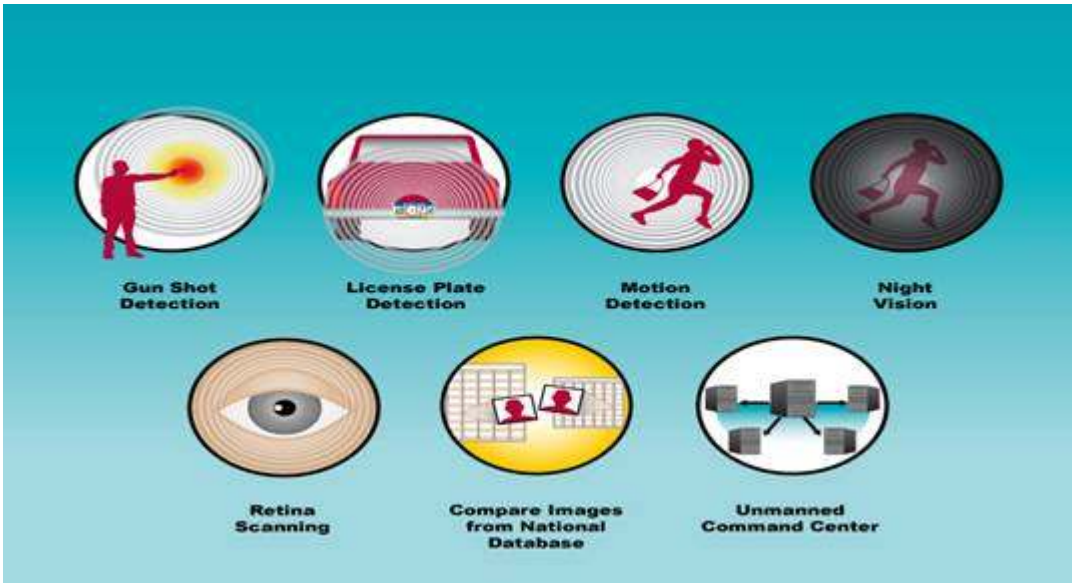


Figure 1: General Characteristics of a Surveillance System

THE INITIATIVE AND ITS CHALLENGES

The City of Pittsburgh is comprised of ninety distinct neighborhoods divided by hilly terrains and wide rivers. Because of its unique and challenging landscape, Pittsburgh's ability to proactively monitor and track suspicious behavior can be a daunting task [26]. To address this challenge and to reduce crime, the Mayor committed to construct and deploy a fully-functional surveillance system, one that can deter crime and provide recorded evidence after a crime is committed [24].

The scope of a city-wide surveillance system is significant. It is estimated that each city neighborhood and business district requires eight to ten cameras to cover a targeted area. Therefore, to cover all ninety Pittsburgh neighborhoods, between 800 to 1,000 cameras are needed. The multitudes of cameras are linked together into one comprehensive surveillance system utilizing a geographical information system (GIS) and sophisticated video analytics to retrieve and analyze data. Besides the logistical challenges of mounting and maintaining the physical equipment, city technology officials need to store and retrieve the vast amounts of data that is continuously accumulated on a 24/7 basis. These capacity concerns are further complicated by the fact that surveillance footage must be retained for several days, potentially consuming many terabytes of data. Thus, maintaining a thousand-camera system is a monumental technical and financial undertaking.

Fortunately, in the fall of 2007, the City of Pittsburgh received a federal Homeland Security grant of nearly $3 million to place surveillance cameras at its bridges, ports and rivers [14, 15]. This federal initiative was designed to allow government officials to monitor and protect navigational points of entry from potential terrorists. By leveraging the technological benefits derived from the placement of cameras obtained from this grant, the City was able to expand its infrastructure into many of Pittsburgh's neighborhoods.

STAKEHOLDERS AND PRIVACY POLICY

Obtaining local government approval for a surveillance project proved difficult. A Pittsburgh councilman, concerned with the civil liberties of the citizenry, demanded that a comprehensive privacy policy be adopted before a single camera could be installed [24]. Such a policy had to thoroughly outline the circumstances for viewing, storing and retrieving data. Ultimately, the privacy policy would prove to be the "backbone" of a successful surveillance project. In addition, it was necessary that all "definitive" stakeholders (using Mitchell et al.'s typology [25]) be involved, or at least considered, in the development of such a policy.

From the very beginning, the development of a privacy policy became a thorny issue. There was significant friction between those who believed that surveillance cameras in the public right-of-way served as a deterrent to crime and those who believed that the existence of even one camera was an invasion of privacy. Proponents believed that a person has no expectation of privacy when cameras are in plain sight or on public property. In other words, the public should not have expectations of anonymity on the public streets and business districts in which they shop and visit each day. On the other hand, civil libertarians believed any surveillance, whether covert or overt, constituted a violation of a person's basic right to privacy and that it represented a "slippery slope" that could lead to additional cameras or more serious types of privacy intrusions.

To address these issues, a committee was established, comprised of representatives from the City of Pittsburgh's law department, its information technology department, the Mayor's office and City Council. The committee's mission was simple and straight-forward: (1) to review the privacy policies of other cities; (2) to understand the technological capabilities of a surveillance system; (3) to determine data retention and access permissions (4) to determine how to obtain city and community group support (stakeholder identification) and approval, and (5) to recommend how to handle organizations and community groups that maintain or want to install their own surveillance systems.

STRUCTURED STAKEHOLDER SELF-IDENTIFICATION PROCESS

The public management literature suggests that for policy development, the most important stakeholders need to be identified (e.g., "definitive" stakeholders in Mitchell et al.'s terminology [25]). Therefore, the key question became how to identify all the stakeholders that would be affected by the deployment of a sophisticated public surveillance system in the City of Pittsburgh. Some initial stakeholders were quickly identified by the committee as shown in table 1. Others were less obvious. Also referred to as "action channels" [23], these influential stakeholders often will require the attention of the project's decision-maker or project committee person and can have a direct role in influencing a project. For instance, understanding that a bureaucrat has "the ear" of a major player within an organization – whether that player is a trusted advisor, an interest group, or a political party – contributes to a prediction and explanation of that bureaucrat's influence. Still, there was a serious concern that an important actor would accidentally be left out. To address this issue, and after several discussions, an innovative approach named, for the purpose of this paper, as "structured stakeholder self-identification" was developed and used. Stakeholder self-identification (i.e. voluntary appearance of a stakeholder) has long been recognized as one of the ways in which to get to know potential stakeholders and some techniques to get public participation have been proposed [40, 6]. More recently, public participation techniques have been refined according to the availability of new media and related techniques [7]. This study proposes applying this knowledge and experience in public participation to the deployment of public IT innovation that is, using techniques from the public participation literature in a systematic way, to get potential stakeholders to identify themselves and then to classify them according to Mitchell et al.'s typology to assess their importance [25]. It is important to emphasize once again that although stakeholder management and public involvement both have long separate traditions in public administration, in particular in projects involving natural resources [6, 18]; they have not been systematically integrated with Mitchell et al.'s stakeholder identification theory [25] for the purpose of timely stakeholder identification in the public sector and even less for the planning and deployment of public information systems. A quick review of six major current textbooks in public management information systems showed that similar to our previous review of non-profit and public management books, although all of them stated the need to perform a stakeholder analysis, they all recommended the formation of a suitable committee for the stakeholder identification process. Consistent with these recommendations, an ad-hoc committee helped to identify the initial group of potential stakeholders and their stake claim in the City of Pittsburgh surveillance system project as shown in Table 1.

Table 1: Stakeholders Initially Identified

Stakeholder	Nature of Stakeholder Interest
City of Pgh Housing Authority	to use City cameras
Hospitals	to rent hospital roof-tops for antennas
Board of Education	to use City cameras
Universities	to use City cameras
Central Business District	to use City cameras for Security & events
Mayor	to protect City from crime
City Council	to protect City neighborhoods from crime
Constituents/Public	to protect City from crime
Community groups/organizations	to protect City from crime
Public Safety Officials (police/fire/EMS)	to assist public safety officials perform job
District Attorney	to serve as an investigative tool
Coast Guard	to protect waterways and rivers
Media	to collect/disseminate info. to the public
City's Chief Information Officer	to design infrastructure/manage project
Technologists	to design infrastructure
Vendors	to sell product
Civil liberty groups	to protect civil liberties
City lawyers	to prepare contract & ensure compliance

Although this study also advocates the use of committees for initial stakeholder identification, it proposes that this approach alone is insufficient to capture the diversity of potential stakeholders in the deployment of a novel IT and for this reason it must be complemented with the proposed structured stakeholder self-identification process. This approach has been developed from a combination of the extant literature of public participation theory and practice and the stakeholder identification theory [25]. The principle of public participation holds that those who are affected by a decision have a right, as a matter of fairness to be involved in the decision-making process. Furthermore, public participation implies that the public's contribution will influence the decision, which is a tenet of deliberative democracy [16]. Still, public participation is not without critics. The main arguments being that the public may fail to understand technical information, particularly risk and uncertainty factors, adequately, may not be able to achieve objective fairness, and that this may lead to trivial results based on a weak consensus among stakeholders [9]. However, what is clear is that new advances in information systems, particularly in social media, make it very easy for stakeholders to organize themselves and to protest, oppose, and even lead to the closure of projects perceived (fairly or not) pernicious for the public [39]. So, whether it is to improve the chances of project success via public acceptance or out of consideration for fairness and democratic principles, it makes sense to involve stakeholders early in the decision-making process using public participation techniques. The practice of public participation provides a set of techniques to communicate with the people who have an interest in the project. Furthermore, public participation techniques distinguish between communication "*to the public*" and "*from the public*" [7]. Using these established public participation techniques [7], the City of Pittsburgh shared the surveillance system initiative "*to the public"* at large through different channels and in different formats as recommended by Creighton [7] and shown in Table 2. The goal was to reach all possible individuals and groups in the community and to invite them to self-identify as stakeholders in the IT initiative.

Table 2: Means of Dissemination of Information TO and FROM the Public

Getting Information FROM the public	Getting Information TO the public
Advisory groups & task forces	Briefings
Appreciative inquiry summit	Exhibits & Displays
Beneficiary assessment	Feature stories
Charrette	Information Repositories
City walk	Internet
Coffee klatch	Mailing out key technical reports
Computer-aided negotiations	Mass mailings
Consensus building	Media interviews
Facilitation	Media kits
Field Trip	News conference/media briefing
Focus groups	Newsletters
Future Search	Newspaper inserts
Groupware	News releases
Hotlines	Paid advertisements
Internet	Panels
Interviews	Presentation to comm. Groups
Large/small group meetings	Public service announcements
Meetings/hearings/workshops	Symposia
Multi-attribute Utility analysis	
Open house	
Participatory rural appraisal	
Participatory technology assessment	
Plebiscite	
Polls and surveys	
Public hearings	
Public meetings	
Retreat	
Samoan circle	
Sarar	
Task force	
Town meetings	
Visioning	
Workshops	

Next, following public participation practices [7], a series of communication activities to retrieve information *"from the public"* and allow new stakeholders to identify themselves and participate in the process were also implemented, as shown in Table 2. These two steps of reaching *"to the public"* in search of potential stakeholders and getting information back *"from the public,"* mainly from self-identified stakeholders constitutes the core of the stakeholder self-identification approach proposed in this paper.

As part of the process the City gave nearly twenty media interviews to publicize the surveillance project and publicly invited potential stakeholders to identify themselves. The City followed the public participation guidelines (Table 2) as a checklist to proactively get information "to" and "from" the public. This approach proved very fruitful. For example, a civil liberties group known as The Constitution Project identified itself as a stakeholder that had a keen interest in protecting the privacy of the public. Without the assistance of the media, this stakeholder would have "fallen through the cracks" and would not have been identified.

What was interesting about the process was that prior to contacting the public, a huge cross-section of stakeholders had been identified. The surveillance system committee, comprised of different groups that represented many varying interests, believed that all possible

stakeholders had been considered. After all, following recommended practices in citizen involvement management [7] there was representation on the committee from social and political groups and technologists alike. However, the structured self-identification approach allowed the identification of new and, in many cases, unexpected stakeholders as shown in Table 3. This table shows the additional stakeholders uncovered by the self-identification process who were not identified in the initial study of the policy committee. In this case, the described "structured stakeholder self-identification" process provided the means for these unexpected stakeholders to participate in the development of the privacy policy and enabled to City to get their backing in the deployment of the surveillance system.

Table 3: Stakeholders that Self-Identified

Stakeholder	Comment
Non-profits (YMCA)	To use City cameras
Banks	To use City cameras
Hotels	To use City cameras
Foundations	To offer funding for additional cameras
Universities	To use camera images for research purposes
Museums/libraries	To use City cameras
Highmark Health Care	To use City cameras
Non-City riverfront areas	To use City cameras
Fraternal Order of Police	To avoid excessive oversight of police work
Grant writers	To assist in obtaining future funding

One example of an unexpected stakeholder and critic of the surveillance system was the *Fraternal Order of Police* (police union). It was rather surprising that they would demand a voice in the deployment plan especially since their main concern was the potential for the City to use the surveillance system to scrutinize the police force! Another unexpected proponent and stakeholder of the city-wide surveillance project was Carnegie-Mellon University (CMU), an important and influential higher-education institution in Pittsburgh. Early in the process, this major research institution approached the city with the hope of obtaining access to some of the surveillance footage from the hundreds of cameras throughout the City of Pittsburgh. CMU was hoping to use these cameras for research and development purposes, and believed that its students could develop new ways of searching and sorting video images from the abundance of data collected by the City. In the end, the City agreed to provide the footage for research purposes only, provided that Pittsburgh's City-Council would amend its camera/privacy policy for such uses. As a result, CMU became a strong and visible partner with the City in obtaining the approvals and acceptance of its many stakeholders. Interestingly, these unexpected self-identified stakeholders proved to be instrumentalin obtainingtheapprovalsforthesurveillance project.

By applying Mitchell's typology of stakeholder identification, it is evident that many of the stakeholders who were not initially identified during the early phases of the project proved to be significant stakeholders. In fact, half of the ten stakeholders that eventually self-identified were categorized as "dominant" or "definitive", that is, they were key stakeholders for the surveillance system (Table 4).

In summary, the "stakeholder self-identification" approach proposed here allowed many unexpected stakeholders to participate in the surveillance system deployment. As a result, the final number of stakeholders was far larger than anticipated.

Table 4: Mitchell's Typology of Stakeholder Identification Applied to the Deployment of Surveillance Technology in the City of Pittsburgh

#	Stakeholder	Power	Legitimacy	Urgency	Type
1	Non-profits		X		2 - discretionary
2	Banks	X	X		4 – dominant
3	Hotels		X		2 – discretionary
4	Foundations	X	X		4 – dominant
5	Universities	X	X		4 – dominant
6	Museums/libraries		X		2 - discretionary
7	Major Healthcare Provider	X	X		4 - dominant
8	Non-City riverfront areas		X		2 – discretionary
9	Fraternal Order of Police	X	X	X	7 –definitive
10	Grant writers		X		2 - discretionary

DEVELOPMENT OF PRIVACY POLICY

To begin, the committee researched and reviewed the privacy policies of several cities, from Chicago to London. Surprisingly, many cities with surveillance systems did not maintain privacy policies, while others refused to release their policies on the basis of confidentiality. Some cities suggested that they were unwilling to deal with the politics of adopting a policy or did not want to be forced to adhere to the terms and condition of a strict privacy policy [26]. Of the cities that maintained a written policy and were willing to share it with Pittsburgh, many focused only on the technical issues, such as capacity of system. Noticeably absent in many of these policies were the civil liberties safeguards that seemed most salient to Pittsburgh's City Council.

Once data from other cities were obtained and reviewed, the committee considered the desired capabilities and functionalities of the surveillance system. Because of federal wire-tapping regulations, it was easy to dismiss systems that record a person's conversations. Next, mainly because of human resources and financial and legal concerns, the City determined that a continuously monitored and staffed command center would not be feasible or affordable. The system would employ sophisticated artificial intelligence, known as video analytics, to determine when to begin filming activity. The system would be programmed to identify suspicious activity, such as a physical attack, spontaneous noise or the placement of a suspicious package unattended in a public space. When such a triggering event would occur, the system would begin to record the conduct and simultaneously alert public safety officials of a possible incident. The officials could review the activity on a computer monitor, transmit the images to mobile data terminals in police cars, and dispatch the police to investigate, if appropriate (Figure 1).

Another issue that needed to be addressed was the retention and accessibility of data. The surveillance system was intended to detect and deter criminal behavior for future use, not to provide evidence in a civil dispute such as a car accident or a suspected cheating spouse. In other words, stored footage lacking evidentiary value would be destroyed so that a person's constitutional rights are not violated [8, pp. 26]. As a result, the committee decided that all recorded data, unless intentionally saved for evidentiary purposes, would be permanently destroyed by being written over every fifteen days. Therefore, even if a judge demanded the release of this data, the City of Pittsburgh could not make it available since it would no longer exist.

The committee, now including all of the identified stakeholders, then considered the multitude of neighborhood groups, community organizations, and businesses that maintain or might desire to install independent surveillance systems. Since many of these organizations receive City monies through grants, it was determined that they would have to adhere to the adopted policy if any government money was used to install or maintain their systems. In other words, unless an organization funds a surveillance project completely independent of government funding, it is required to provide the same privacy safeguards as the City. To ensure compliance, a group's executive director or leadership board would have to sign a statement and release the City of liability from abuse or misuse of the surveillance system, acknowledging and agreeing to the terms and conditions of the City of Pittsburgh's approved privacy policy. The policy further provides that the City may not review footage captured by independent cameras unless the organization has signed such a statement.

The committee also dealt with the issue of how to best obtain the blessings and approvals of City-Council and local community groups. This was done by engaging all identified stakeholders including civil liberties groups such as the ACLU and The Constitution Project, a Washington, D.C.-based civil liberties organization. Before the policy would be presented to City-Council for approval, these groups would have an opportunity to review and provide input, which they did.

Approximately nine months after Pittsburgh's City Council demanded a privacy policy, a draft of the policy was written. During these nine months, the City held a fact-finding public meeting, known as a post-agenda, with the identified stakeholders including industry experts and representatives from various community and civil liberties groups to discuss the nuances and feasibility of the proposed policy. A second public meeting was subsequently scheduled to obtain input and reaction from the general public. These public meetings brought representatives from the community, civil liberties groups, the City's public safety department, and various media outlets together. These meetings and hearings resulted in a clearer understanding, by the surveillance system stakeholders, of the policy's intent, protections, signage, training requirements, and penalties for violations while providing an additional avenue for interested stakeholders to come forward and self-identify.

Finally, after a year of meetings, hearings, and discussions, the City of Pittsburgh passed one of the most comprehensive privacy policies in the country. In the words of the Director of the Greater Pittsburgh chapter of the ACLU, this policy "is about as good as it can be" [14].

RFP PROCESS AND AWARD/CONTRACT DECISION

Once the privacy policy was adopted, the City of Pittsburgh was ready to tackle the difficult task of choosing a vendor and building the system. Once again, transparency and procedure had to prevail to ensure the retention of the stakeholders' trust and support. The opportunity to bid on a project of this magnitude had to be offered to any responsible company capable of offering these services and, therefore, a Request for Proposal (RFP) was written. The RFP asked interested vendors to design the video-analytics, configure the band-width requirements, determine data storage capabilities, and outline an installation schedule for this project. In order to ensure objectivity and transparency, a three-pronged approach was devised. First, hire an objective consultant that had experience preparing and evaluating surveillance systems, writing RFP's, and evaluating surveillance projects. Second, assemble a review team to sift through the RFP responses. Third, form a selection committee representing stakeholders from Pittsburgh's administration, elected officials, and Homeland Security representatives.

The RFP provided for an initial five-week response period, but was soon extended for an additional four weeks to allow vendors to conduct site tours, and to configure and estimate the project's cost and scope. At the end of the period, there were nine proposals submitted from firms across the country, with many of the respondents having experience in designing and implementing similar systems throughout the country.

Four separate entities evaluated these nine proposals independently. These entities included the administration's project manager, the outside consultant that prepared the RFP, a third party technology company consisting of former computer science professors familiar with emerging surveillance technologies, and the City of Pittsburgh's information technology department. Each body independently reviewed proposals and ranked each according to its cost, design, implementation schedule, and vision.

Of the original nine respondents, four vendors provided the most efficient and cost effective solutions. To ensure a fair and transparent process, one-hour interviews were scheduled with each finalist. The interviews were scheduled to take place in a day-long marathon session with representatives from the original selection committee present to hear the proposals. The interviews took place in the Mayor's private conference room with the Mayor himself attending the presentations. After a marathon session with the four finalists, the committee selected a winning vendor. Next, a contract was crafted to identify the system deliverables and timetable, including a detailed minority and woman's business enterprise (MBE/WBE) participation strategy [26]. After holding six weeks of contract negotiations and obtaining the requisite administrative approvals, a contract was finally in place.

INSTALLATION OF THE PUBLIC SURVEILLANCE SYSTEM

Nearly fifteen months after receipt of the original application for a Homeland Security grant, a comprehensive privacy policy was adopted and a signed vendor contract was completed; Pittsburgh was finally ready to begin installing cameras. The first order of business was to obtain government permits and private sector permissions to mount the cameras on telephone poles and high-rise buildings. City engineers and

inspectors needed to make sure the telephone poles and street lights were strong enough to support the equipment. The camera installation schedule needed to address traffic concerns and to minimize roadway blockages. Finally, city planners and historic preservationists got involved to ensure the camera design met the city's aesthetic requirements.

Due to line-of-sight requirements for this wireless initiative, permissions from building owners to place cameras on their privately owned rooftops required landlords and city lawyers to get involved. Some property owners were satisfied with simple liability releases protecting them from damage to their proprieties, while others demanded significant compensation for the use of their rooftops. Again, city lawyers and finance procurement specialists needed to negotiate long term leases. Once these logistical issues were resolved, public safety personnel needed to determine camera location. Analyzing neighborhood crime trends, coupled with community interest, helped to identify appropriate placement.

Figure 2: Installed Camera in the City of Pittsburgh

After the bureaucratic obstacles and stakeholder concerns were addressed, the first surveillance camera was installed (Figure 2). From installing and configuring the software, to ordering and mounting the hardware, it took only four weeks to make the system operational. Since its initial deployment, more than 22 city-owned cameras have been installed and have helped solve some very high profile crimes in Pittsburgh [37].

DISCUSSION AND LESSONS LEARNED

When this initiative began, a great deal of energy was spent planning this project and identifying the key stakeholders. It was clear that for this project to succeed, it would be necessary to include any and all people or organizations that might have a vested interest in the public surveillance system. In other words, all relevant stakeholders must be identified.

The challenge, however, was how to identify all valid stakeholders in the context of the public surveillance system. The solution was to develop and use a "stakeholder self-identification" approach that, using the theory and practice of stakeholder management and public participation, systematically publicized the initiative and invited all potential stakeholders to identify themselves. For this, public participation techniques to convey the message "to the public" and to receive input (self-identification) "from the public" were put in place. There was a multiplicity of self-identified stakeholders, some of them totally unexpected, who stepped forward, ranging from civil libertarians (mostly concerned with privacy issues) to the Pittsburgh police union (which wanted to protect their membership from continuous scrutiny and potentially constant video review of their officers' conduct in the field). These stakeholders were sorted according to their importance (although not used at the time of the case, Mitchell et al. [25] provides the best framework for stakeholder classification and is the one recommended in the proposed self-identification approach).

Although the policy committee tried to identify all of the potential stakeholders according to sensible assumptions and expectations (see Table 1), the final tally of stakeholders, after using the proposed self-identification process, was not only larger but included some surprising "key" participants such as the Fraternal Order of Police (police union) as mentioned earlier (see Table 4) and "key" action channels [23] that the appointed policy committee failed to consider but who ultimately influenced the outcome of the project.

In conclusion, the self-identification process proposed in this research can be summarized as follows:

Step 1 – Set up a steering group to identify the initial stakeholders and to manage the process [5]

Step 2 – Use public participation techniques, in a systematic way, to communicate the IT deployment highlights "to the public" and invite potential stakeholders to stand up and identify themselves [7]

Step 3 – Use public participation techniques, in a systematic way, to ensure communication "from the public" (self-identified stakeholders) to the steering group to allow its claim validation [7].

Step 4 – Use Mitchell et al.'s Stakeholder Salience and Identification framework to validate the stakeholders' claims, in terms of their salience and importance (dormant, discretionary, demanding, dominant, dangerous, dependent, and definitive) [25, Appendix A].

Step 5 – Develop a strategy to allow participation of the identified stakeholders according to their type, paying particular attention to the claims of those who are definitive stakeholders [25, Appendix A].

The case discussed here validates the wisdom of using this five-step "structured stakeholder self-identification" process where many of the salient stakeholders self-identified using the approach proposed in this paper. The key argument in this paper is that public IT innovations make the task of identifying stakeholders very difficult while the proposed "structured stakeholder self-identification" increases the likelihood of locating more relevant stakeholders. Furthermore, even in the case that a key stakeholder was not identified, the public "best effort" made by the City would certainly contribute to goodwill by the parties. This argument can be illustrated with an example of what might have occurred if the proposed structured approach to identify stakeholders had not used.

THE PERILS OF UNIDENTIFIED STAKEHOLDERS

Identifying stakeholders and addressing their concerns early in an IT initiative is not only important for large IT projects. Even those technology ventures that are much smaller in scope require policy makers to identify the salient participants. An example of how the failure to identify salient stakeholders can be problematic can be illustrated by the Wi-Fi initiative of the Pittsburgh Downtown Partnership (PDP). Funded by local businesses and property owners, the PDP is committed to a central business district that is clean, safe and inviting for economic development opportunities. The goal, of course, is to develop and encourage a thriving business environment in the downtown area of Pittsburgh. This non-profit organization sought permission from local government officials to use the City's publicly owned utility poles and street right-of-ways to construct a mesh network offering wireless services within the central business district. This network would provide downtown businesses, residents, students and visitors an opportunity to access a wireless network for emails or file sharing. PDP considered the City local government as their only salient stakeholder (i.e. once approved by the City, they would deploy the wireless access). Obtaining approvals from the local government however, proved to be very controversial. Once word got out PDP had requested city officials to approve the use of public resources for this project, numerous unexpected stakeholders began to emerge. What initially started as a straight-forward, "rubber stamp" approval process turned out to be a somewhat controversial media event. Since the PDP did not initially consider and address the concerns from vendors, residents and fiscal specialists, a seemingly simple approval process turned out to be a difficult and time consuming exercise in bureaucracy, negotiations, and politics with these unexpected stakeholders (more details on this problematic initiative appear in Appendix B). If the PDP had identified the salient stakeholders earlier, an easier and more transparent approval process could have occurred.

CONCLUSION

This study has a two-fold contribution. First, from a theoretical perspective, it contributes to the IT public management literature by proposing the use of a normative structured approach toward eliciting voluntary stakeholder self-identification on a timely basis. To date, stakeholder self-identification had been accepted as a possible way to identify stakeholders, but its use has been mainly restricted to the public management of natural resources [18]. This study combines Mitchell et al.'s seminal work [25] on stakeholder identification theory with well-known techniques from the public participation literature [7]. Second, and from a practitioner's perspective, it provides public IT managers with a normative framework for public salient stakeholder identification and assessment, as well as minimizes the risks of failing to identify stakeholders (even if a

stakeholder is not identified, it can be openly demonstrated that it was not for the lack of trying).

In addition, there is also a moral argument supporting the proposed structured stakeholder self-identification process which relies heavily on getting stakeholders to participate in IT deployment/planning and policy using public participation techniques. This moral argument is based on the first core value of public participation which states that those who are affected by a decision have the right to be involved in the decision-making process [21]. This statement is particularly valid in a public information system funded by the public which will be used and/or affected by the public [27].

However, public involvement can also involve potential risks and pitfalls and for this reason it is important to decide when and to what degree public participation is desired [12, 35]; therefore, exploring and providing guidelines about how the participatory processes should take place would certainly help to implement the proposed structured stakeholder identification approach effectively. As a final note, the approach proposed here certainly contributes to openness and transparency which are very important in the implementation of any public IT initiative, and facilitates a wide acceptance of public information systems in the public sector.

REFERENCES

[1] Allen, W. and Kilvington M. "Stakeholder Analysis", http://www.landcareresearch.co.nz/research/social/stakeholder.asp, September 10, 2010.

[2] Baker, A. "More Tech Tools for the Terror Fight." *The New York Times,* May 20, 2010.

[3] Bozeman, B. and Bretschneide S. "Public Management Information Systems: Theory and Prescription," *Public Administration Review,* Volume 46 (Special Issue), 1986, pp. 475-487.

[4] Buchholz, R. A. and Rosenthal S.B. "Stakeholder Theory and Public Policy: How Government Matters." *Journal of Business Ethics* Volume 51, Number 2, 1994, pp. 143-153.

[5] Bryson, J. M. *Strategic Management for Public and Non-Profit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement. 3rd Edition*, Jossey-Bass, San Francisco, 2004.

[6] Creighton, J. L. (1983). Identifying publics/staff identification techniques. In J.L. Creighton, J. Delli Priscoli, and C. Mark Dunning (Eds), *Public involvement techniques: a reader of ten years' experience at the Institute for Water Resources*, IWR Research Report 82-R1. Fort Belvoir, VA, Institute for Water Resources, U.S. Army Corps of Engineers.

[7] Creighton, J. L. *The Public Participation Handbook: Making Better Decisions Through Citizen Involvement*, Jossey-Bass, San Francisco, 2005.

[8] The Constitution Project 2007. *Guidelines for Public Video Surveillance*. Washington, D.C.

[9] Dietz, T. and Stern P.C. *Panel on Public Participation in Environmental Assessment and Decision Making*, The National Academies Press, Washington, D.C., 2008.

[10] Freeman, R.E. *Strategic Management: A Stakeholder Approach*, Pitman, Boston, 1984.

[11] Freeman, R.E., Harrison, J.S., Wicks, A.C., Parmar, B.L., and DeCole S. *Stakeholder Theory: State of the Art*, Cambridge University Press, Cambridge, MA, 2010.

[12] Glicken, J. "Getting Stakeholder Participation 'Right': A Discussion of Participatory Processes and Possible Pitfalls," *Environmental Science & Policy*, Volume 3, 2000, pp. 305-310.

[13] Gregory, R. and Keeney, R.L. "Creating Policy Alternatives Using Stakeholder Values," *Management Science*, Volume 40, 1994, pp. 1035-1048.

[14] Gurman, S. "City to Keep and Electronic Eye on Crime Developing Camera System with Help of $2.6 million Homeland Security Grant," *Pittsburgh Post-Gazette*, September 21, 2008.

[15] Gurman, S. "Keeping an Eye on Crime: Pittsburgh Developing Camera Network to Peer Down on Waterways, Bridges," *Pittsburgh Post-Gazette*, September 21, 2008.

[16] Gutmann, A. and Thompson, D. *Why Deliberative Democracy?*, Princeton University Press, Princeton, NJ, 2004.

[17] Harrison, J.S. and Freeman, R.E. "Stakeholders, Social Responsibility, and Performance: Empirical Evidence and Theoretical Perspectives," *Academy of Management Journal*, Volume 42, Number 5, 1999, pp. 479-485.

[18] Heathcote, I.W. *Integrated Watershed Management: Principles and Practice, 2nd Ed.*, John Wiley, Hoboken, NJ, 2009.

[19] Hofman, H.F., Lehner, F. "Requirements Engineering as a Success Factors in Software Projects," *IEEE Software*, July/August 2001, pp. 58-66.

[20] Hulse, C. "Threats and Responses: Plans and Criticisms: Pentagon Prepares a Future Market on

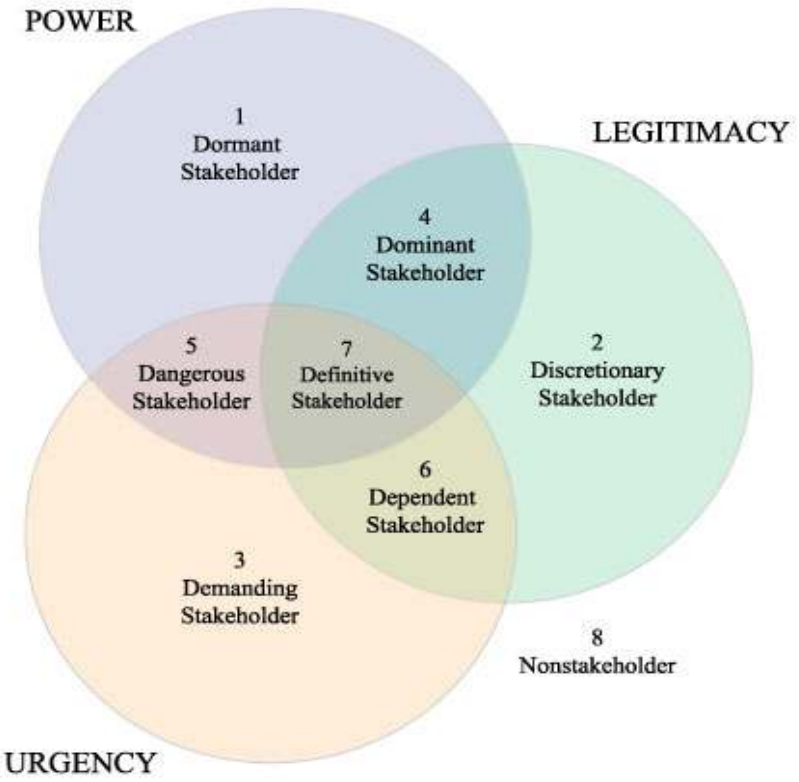
Terror Attacks," *The New York Times*, July 29, 2003.
[21] International Association for Public Participation. "IAP2 Core Values," http://www.iap2.org/displaycommon.cfm?an=4, September 28, 2010.
[22] Kaminer, A. "Has the Big Apple Become the Big Eyeball?" *The New York Times*, May 7, 2010.
[23] Karsner, S.D. "Are Bureaucracies Important? (Or Allison Wonderland)," *Foreign Policy*, Volume 7, 1972, pp. 159-179.
[24] Lord, R. "Council OKs Surveillance Cameras Around City," *Pittsburgh Post-Gazette*, September 20, 2007.
[25] Mitchell, R.K.. and Agle, B.R. "Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts," *Academy of Management Review*, Volume 22, Number 4, 1997, pp. 853-886.
[26] Moorer, F. Surveillance System Project Manager, City of Pittsburgh, interview with author, June 13, 2010.
[27] Orman, L.V. "Public Information Systems," *Information and Society*, Volume 6, Number ½, 1989.
[28] Pan, G.C. and Flynn, D. "Information Systems Project Abandonment: A Case of Political Influence by the Stakeholders," *Technology Analysis & Strategic Management*, Volume 15, Number 4, 2003, pp. 457-466.
[29] Perrow, C., *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, NJ, 1999.
[30] Rawlins, W.L. "Prioritizing Stakeholders for Public Relations," White paper, Institute of Public Relations, www.instituteforpr.org, September 10, 2010.
[31] Rocheleau, B., *Public Management Information Systems*, Idea Group Publishing, Hershey, PA, 2005.
[32] Slobogin, C., *Privacy at Risk: Surveillance and the Fourth Amendment*, University of Chicago Press, Chicago, IL, 2007.
[33] Sundgren, B. "What Is a Public Information System?" *International Journal of Public Information Systems,* Volume 2005, Number 1, 2005.
[34] Swain, J.W., White, J.D. and Hubbert, E.D. "Issues in Public Management Information Systems," *The American Review of Public Administration*, Volume 25, Number 3, 1995, pp. 279-296.
[35] Thomas, J.C. "Public Involvement in Public Management: Adapting and Testing a Borrowed Theory," *Public Administration Review*, Volume 50, 1990, pp. 435-445.
[36] Thompson, J.D. *Organizations in Action*, McGraw-Hill, New York, 1967.
[37] Vidonic, B. "Pittsburgh Safety Officials Tout Network of Cameras," *Pittsburgh Tribune-Review*, August 5, 2010.
[38] Vos, J.F. "Corporate Social Responsibility and the Identification of Stakeholders," *Corporate Social Responsibility and Environmental Management,* Volume 10, Number 3, 2003, pp. 141-152.
[39] Wasik, B. "Crowd Control", *Wired*, January 2010, pp. 76-112.
[40] Willeke, G. E. "Identifying the Public in Water Resource Planning", *Journal of Water Resources Planning and Management Division* (American Society of Civil Engineers), Volume 102, Number 1, 1976, pp. 137-150.

AUTHOR BIOGRAPHIES

Enrique Mu, Ph.D. is MBA Program Director at Carlow University and Director of the Summer Training Program for Latin American Executives (PROCAGE) at the University of Pittsburgh. His research interests are in the areas of IT management, managerial cognition, decision making, and effective use of Information Technology in organizations. He was recently awarded a proclamation by the City of Pittsburgh for leading the decision-making process to select a suitable Cloud Technology for the city.

Howard A. Stern, Ph.D. served as the Chief Information Officer for the City of Pittsburgh from 2004 to 2012. In 2011, he was named CIO of the Year by the Pittsburgh Technology Council. Dr. Stern is currently the Associate Dean of Academic Administration and Assistant Professor of Management at Carlow University in Pittsburgh. His research interests include the relationship between politics and technology, e-government, e-discovery and social media.

APPENDIX A



Dormant Stakeholders – "possess power to impose their will on a firm, but by not having a legitimate relationship or an urgent claim, their power remains unused."
Discretionary Stakeholders – "possess the attribute of legitimacy, but they have no power to influence the firm and no urgent claim."
Demanding Stakeholders – "those with urgent claims but having neither power nor legitimacy, are the "mosquitoes buzzing in the ears" of managers."
Dominant Stakeholders – "their influence in the firm is assured, since by possessing power with legitimacy, they form the 'dominant coalition' in the enterprise."
Dependent Stakeholder – "who lack power but who have urgent legitimate claims as 'dependent,' because these stakeholders depend upon others (other stakeholders or the firm's managers) for the power necessary to carry out their will."
Dangerous Stakeholders – "Coercion" is suggested as a descriptor because the use of coercive power often accompanies illegitimate status.
Definitive Stakeholders – "a stakeholder exhibiting both power and legitimacy. When such a stakeholder's claim is urgent, managers have a clear and immediate mandate to attend to and give priority to that stakeholder's claim."

APPENDIX B

THE PERILS OF UNIDENTIFIED STAKEHOLDERS: A WIRELESS DOWNTOWN

The Pittsburgh Downtown Partnership (PDP) initially thought that issuing a request for proposal (RFP) for a wireless downtown infrastructure and soliciting bids and funding would be the most challenging part of this process. Unfortunately, that was not the case. Instead, obtaining the necessary permits and government permissions proved to be the most challenging part of the process. The PDP soon discovered that the use of publicly funded assets requires a public vetting and approval process. Inherently designed to flush out all relevant stakeholders, this approval process served as a sounding board for all interested participants. Initially reported by the local media, the approval to construct a wireless downtown network soon drew the attention of special interests. Many of these stakeholders were unexpected and took the PDP by surprise. As soon as the story was reported, technologists and elected leaders were complaining that the proposed wireless infrastructure was not sufficient and that revenue opportunities were being lost by not charging a fee for the use of City assets. Although the PDP believed that the economic development opportunities for the downtown areas far outweighed the potential revenue streams for the City, several council members openly discussed the potential financial opportunities. Once the media began discussing these opportunities, additional stakeholders emerged offering opinions about how to proceed.

Because the PDP did not anticipate the backlash from these stakeholders, it had to scramble to convince and respond to council members, technologists, and vendors about the merits of this project. Had the PDP recognized the stakeholders earlier in the process, much of the skepticism and controversy could have been proactively dealt with.

One of the unexpected stakeholders to emerge was the City's public safety personnel. They demanded that any wireless areas in Pittsburgh be made available to the police, fire and emergency medical services personnel at no cost. These public safety officials correctly pointed out that since many of Pittsburgh's downtown fortress-like structures were practically impenetrable due to their thick stone exteriors and size, wireless communications were frequently spotty. Therefore, any system that would use publicly owned assets must be made available to the City's Public safety officials free of charge.

There were also stakeholders that believed that the City should lease its assets to the PDP instead of giving them away for free. These fiscally-concerned constituents believed that a dependable wireless network should not be given away for free and that businesses or consumers should pay for it. This revenue-generating service could be used for the upkeep and repairs of the assets needed to maintain the wireless system.

Finally, there were those skeptics that questioned the technology design itself and warned that the wireless plan was not the best way to provide coverage. These critics believed that there were better and less expensive methods of providing wireless services and that a failed project would cast the City in a negative light on a national stage.

In the end, the Pittsburgh City Council passed the legislation granting PDP permissions to use its street light poles and valuable right-of-ways. Unfortunately, this did not happen before much acrimonious controversy and discussion took place. Those salient stakeholders that emerged later into the project felt they had been left out in the initial discussions on purpose, and remained a source of conflict during the implementation and final deployment. If the PDP had recognized the various stakeholders and dealt with them earlier in the process, the approval process could have gone more smoothly and quickly and the downtown Wi-Fi deployment would have enjoyed a wider and less controversial acceptance.