SmaCCS: Smart Camera Cloud Services
Towards an Intelligent Cloud-based Surveillance System

Sven Tomforde[1], Uwe Jänen[1], Jörg Hähner[1] and Martin Hoffmann[2]
[1]*Organic Computing Group, University of Augsburg, Eichleitnerstr. 30, 86159 Augsburg, Germany*
[2]*Volavis GmbH, Schuckenteichweg. 31, 33818 Leopoldshöhe, Germany*

Keywords: Intelligent Surveillance, Cloud Computing, Automated Machine Learning, Smart Camera, Organic Computing.

Abstract: Today, high performance and feature rich surveillance systems are very costly as they require an expensive set of infrastructure components. As a consequence, such systems including, e.g., complex automatic video content analysis, are restricted to large scale applications, such as airports or train stations. In smaller settings, e.g. in shop surveillance, mostly low-cost display or record-only systems are in use. In this position paper we propose to combine two well-known approaches in order to make Intelligent Video Surveillance applicable and affordable in small to medium-scale scenarios. The proposal includes to combine the concept of Smart Cameras, i.e. cameras equipped with local processing resources, with the ideas of Cloud Computing, i.e. the on-demand provisioning of computing and storage services for complex calculations, and the management of large amounts of data, i.e. video storage. The former allows for the cost effective pre-processing of video data close to the sensor, while using the latter concept does not require large initial investments into expensive infrastructure components such as powerful compute servers. The paper presents research issues of the necessary system design, including precise system goal and system model aspects. Based on this, we discuss several research issues required to be addressed for solving the overall goals.

1 INTRODUCTION

Within the last decade, a strongly increasing usage of video-based surveillance has been observed driven from both, the industry- and academia-side. The application spectrum reaches from analyses of customers' flows in retail business to semi-automated surveillance of safety-critical areas like airports and railway stations. Most of the currently used systems are proprietary and isolated applications serving just one specific purpose. Typically, they consist of a predefined set of cameras and a central point of operation, where all video streams are combined, stored, and observed by human operators. This system model results in non-scalable, hardware-intensive, and consequently cost-inefficient solutions, see e.g. (Javed and Shah, 2008).

One promising solution to alleviate these undesired system properties is to combine Cloud Computing (Vaquero et al., 2008) concepts with more autonomy for the cameras: *Smart Camera Cloud Services* (SmaCCS). The term *Smart Camera* (SC) refers to a standard camera that is equipped with an on-board computation unit which is able to fulfil video preprocessing tasks (e.g. feature extraction and annotation of video files with meta-data). In addition, a variable set of SCs is able to self-organise a surveillance network. Thereby, the Cloud-solution serves as interface to the user and as basis for computation-intensive tasks like video analysis (e.g. detection of persons and movements, see (Jänen et al., 2012)), pattern recognition, and learning of conspicuous and abnormal behaviour. A possibly large set of SCs will most probably result in a huge amount of data that needs specific analyses methods following the *Big Data* principle (Bryant et al., 2008), which is most promisingly tackled using a Cloud-based approach.

This paper outlines the general SmaCCS system and names the upcoming research challenges to be addressed. The paper is structured as follows. Section 2 describes the state of the art regarding Smart Camera and Intelligent Surveillance Systems, followed by concepts for moving parts of the functionality into the Cloud. Afterwards, Section 3 introduces the system design of SmaCCS and highlights the most important research issues. Finally, Section **??** summarises the paper and gives an outlook to current and future work.

Tomforde S., Jänen U., Hähner J. and Hoffmann M..
SmaCCS: Smart Camera Cloud Services - Towards an Intelligent Cloud-based Surveillance System.
DOI: 10.5220/0004590902880293
In *Proceedings of the 10th International Conference on Informatics in Control, Automation and Robotics* (ICINCO-2013), pages 288-293
ISBN: 978-989-8565-70-9

2 RELATED WORK

Intelligent Surveillance Systems and Smart Cameras. According to (Velastin and Remagnino, 2006), intelligent surveillance systems can be classified by their degree of autonomy and capability to satisfy self-X properties like self-organisation and self-configuration. The first class consists of analogues CCTV (Closed Circuit Television) techniques for image distribution and storage in a single control room. In contrast, systems of the second class already combine computer vision and CCTV which results in semi-automatic visual surveillance. Finally, fully automated wide-area surveillance systems represent the third class. These systems are characterised by the distribution of intelligence among a possibly large set of collaborative cameras.

The targeted SmaCCS observation system consists of several pan-tilt-zoom (PTZ) capable Smart Cameras (SC), see Fig. 1. A SC is an automated system and combines an optical sensor with a computation unit for preprocessing and on-board analysis of video data, see (Schneiderman, 1975). The output of the optical sensor is preprocessed by the local computation unit; hence, only limited image data has to be transferred using communication and the network traffic can be mostly reduced to event- and status-messages.

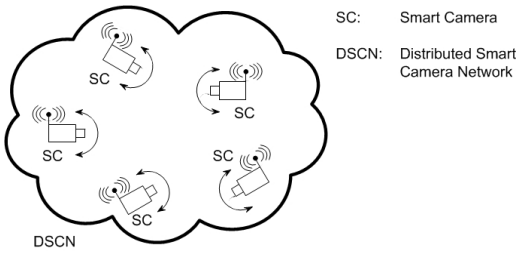

Figure 1: Schematic overview of a SC network.

Surveillance systems have captured increasing interest of both, the research and the industrial worlds, in recent years (Javed and Shah, 2008). In the last decade, surveillance systems of the third class, self-X properties like self-organisation and the distribution of hardware components have been the focus of investigations (Collins et al., 2001; Lipton et al., 2004; Monari, 2012). The gap between research and real robust industrial systems is wide. The initial costs to build up a commercial full-automated surveillance system are very high. Even large cities like London run semi-automated systems, e.g. a static camera is able to detect persons entering forbidden areas, (Cernium, 2013). Nonetheless, great parts of the initially demanded research (Chu et al., 2004) has been successfully performed for pure video surveillance systems. The SmaCCS project aims at closing the remaining gap by reducing the initial costs with a pay-per-use concept and an outsourcing of hard- and software components in the Cloud.

Cloud Computing – Privacy Issues and the Application to Surveillance or SC Systems. Cloud Computing (Vaquero et al., 2008) emerged as a pay-per-use approach for accessing computing resources (hardware and software) that are delivered as a service over a network (i.e. the Internet). In this context, the term "Cloud" describes the virtualisation and abstraction of the potentially complex infrastructure and the remote access by customers. Today, a variety of commercial Cloud-solutions are available focussing on data centre (e.g. Amazon's EC2), storage (e.g. Dropbox), or Software (e.g. Microsoft's Office 365). The focus of the SmaCCS approach is to make use of the data centre functionality as this is an economical (i.e. reduce initial hardware cost) and highly scalable alternative to centralised system architectures of current surveillance systems.

Due to the potentially computation-extensive processing tasks caused by continuous video data from a large set of sources, a scalable Cloud-based computation unit is necessary. Similar ideas have already been presented in the literature. For instance, (Zhang et al., 2009) describe a quality monitoring process in industrial automation that is based on visual inspection (i.e. to detect surface defects). Here, the standard approach is to make use of extensive image logging and off-line human interpretation. In contrast, the authors introduce their concept of measuring micrometer defects from a distance using a cloud of cheap vision sensors.

Besides this first industrial-based video analysis scenario, other researchers worked on a "Cloud-based algorithmic framework which is scalable and adaptive to online smart city video sensing system" (Wen et al., 2010). Here, spatio-temporal relationships are derived from large-scale camera networks and simulated using a Cloud-setup in order to build the best possible topological structure. Hence, the focus is more on design time decision support than on runtime usage of the Cloud as access and analysis platform.

Finally, privacy is an important issue if sensible data is transferred to the Cloud (i.e. in terms of legal compliance and user trust). Therefore, (Pearson, 2009) state that this has to be covered at every phase of designing the system. Corresponding aspects concerning the privacy challenges will be considered within the SmaCCS system.

3 SYSTEM DESIGN

The following section defines the goal and describes the system design of SmaCCS. Afterwards, the corresponding research challenges are outlined.

3.1 System Goal

The goal of SmaCCS is to investigate a scalable system allowing for an affordable semi- or full-automated intelligent video surveillance system. In this context, *affordable* means that the user installs one gateway and as many out-of-the-box SCs as he needs for the specific tasks, let these SCs automatically configure themselves based on the bought license-model, and use a scalable access- and processing-solution in the Cloud. The user will be taxed for the Cloud-part on a pay-per-use approach. The Cloud-based solution reduces the initial investment cost and increases the scalability of the system and the possibility to automatise image-analysis and recording management tasks. The system can consist of arbitrary SCs, whereas the user is taxed on the particularly used number. The system aims especially at small- and medium-sized surveillance tasks, like the observation of business areas, large private households, or railway stations and airfields.

3.2 System Model

The system model consists of a user-side and a Cloud-side. Details are illustrated by Fig. 2. The Cloud's server components are an application-, a Nagios- (Nagios Enterprises, 2013), and a message-queueing (MQ) server. The image-database as well as the Cloud-analysis unit are the core components to perform exhausted image-analysis on Cloud-side. On user-side, the SCs and a gateway to connect to the Cloud have to be installed. The user accesses the observation system as well as the image-analysis results via an application-interface (GUI).

3.2.1 User-Side

As mentioned before, a SC consists of an optical sensor (e.g. a pan-tilt-zoom capable camera), a light-weighted computation unit (SC-analysis), and a communication interface. Each of the SCs is able to perform parts of the image analysis like movement detection and detection of persons. In addition, the SC can observe suspicious events (like persons approaching forbidden areas). Based on this information, the SC decides autonomously about the frame-rate and the image quality to be stored at server-side (within the Cloud) and annotates the video data with the derived meta-information. This reduction of irrelevant information is an important step for image-data-compression which is essential for Cloud-based storing of data.

3.2.2 Cloud-Side

The pre-processed image-data is streamed to the image-database for storing and the Cloud-analysis for post-processing. Based on the annotated data stored in the Cloud's database, the user can perform computational-intensive analysis tasks or search for specific situations (e.g. besides a standard search like "all video data between time a and b", he might look for persons with yellow clothes). The application server is the connection-interface to the user. It processes the image analysis results and presents it to the user. Single SCs communicate via XML messages likewise to the *Sensor Model Language* (SML, 2013). Therefore, the MQ-server is the transferring communication component, as well as the communication between application server and SC network. As the whole system consists of Cloud- and distributed components, it is necessary to capture system states for maintenance services. The Nagios-Server is an adequate solution to handle component malfunctions.

3.3 System Components and Research Challenges

The overall system as outlined in Fig. 2 consists of a variable set of SCs, a Cloud-based server, and a web-based user-access system. The following part of this paper describes the corresponding system components to be developed and the resulting research challenges related to these components.

1. Smart Camera System. SmaCCS builds upon the results of the *CamInSens* system (D'Angelo et al., 2012) and *QTrajectories* project (Jänen et al., 2012). Fig. 3 depicts the data stream within a single SC. The image-data will be transferred from the optical sensor (chip) to the internal-processing unit (PROC) of the camera – this provides a video stream via its communication interface (COMM). Typically, this optical sensor is a standard pan-tilt-zoom camera. In addition, the sensor annotates the current timestamp and current pan-tilt-zoom configuration to the JPEG-header. For hard real-time constraints, this information should be annotated as close to the data source as possible. The SC-analysis unit is responsible for the first image analysis (like person detection). The enriched and annotated image data is accessible via a COMM Interface by the Cloud services.

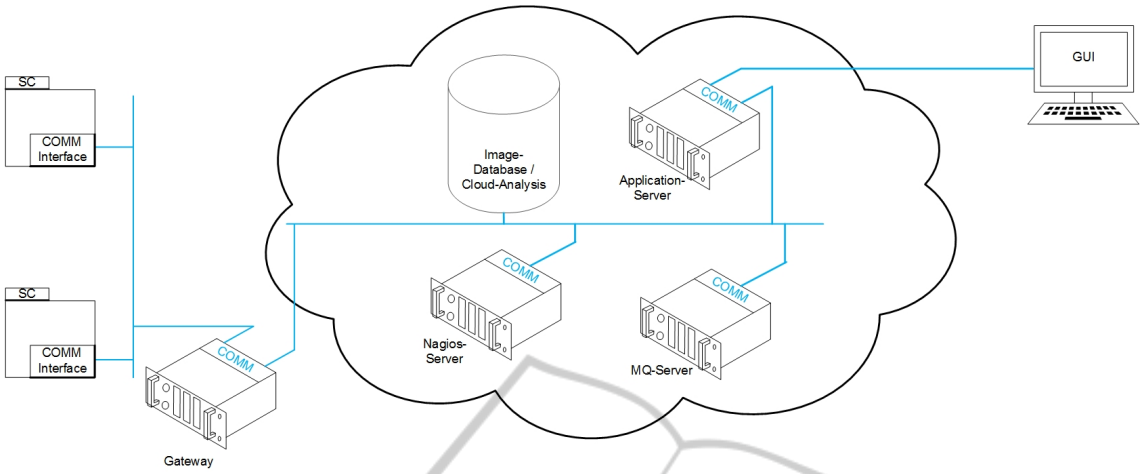

Figure 2: System Model of the SmaCCS system.

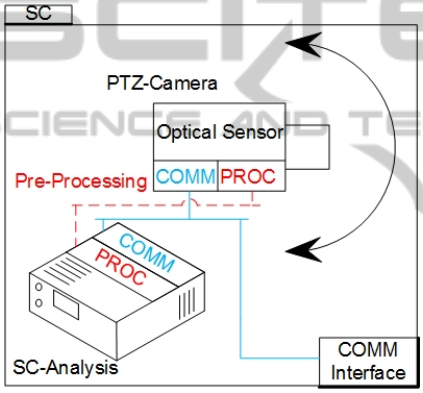

Figure 3: Architectural view of a single SC.

Typical observation jobs (like counting people in an entrance area of a building) are usually fixed assigned to dedicated SCs located at specific positions (e.g. above a door). More sophisticated surveillance jobs like "look at position X"-commands initiated by a user to get an image of a special location, need a more sophisticated job scheduling method. Therefore, each observation job is represented by a software-agent. This agent is responsible for the fulfilment of the user command. Such an observation job can be initiated by the user or by the SC system itself as a reaction to the observation result of another surveillance job. The agent itself searches self-organised for an adequate SC resource to fulfil its job. Therefore, the agents trade camera resources within the system. Another possibility is that more important agents simply suppress other agents from a camera resource.

In addition, the control of each SC can be improved. Thereby, the Multi-level Observer/Controller (MLOC) framework (Tomforde, 2012) will be applied to each SC in order to develop a self-organising camera alignment solution. Furthermore, the MLOC framework serves as classification system for the currently detected situation of the SC and therefore decides about the data-quality to be submitted to the Cloud, similar to the classification of network-traffic situations in (Tomforde et al., 2011).

2. Cloud System. Besides the "normal" technical Cloud-side tasks as outlined before, the main research challenges refer to a) an efficient data-storage solution for video and image data and b) to intelligent data-analysis method (e.g. based on machine learning techniques). Storing video data efficiently and accessing the contents based on a database concept is an interesting task and has attracted researches for years, see e.g. (Collins et al., 2001) for a good overview. Here, the challenge is to provide an efficient technique for searches and queries that scales well with possibly huge data – i.e. as provided by relational databases. Video and image data are not suitable for relational databases – hence, a data partitioning concept is needed. The second part – the Cloud-analysis – has to find best-possible answers to user queries. Thereby, the query should be more powerful than standard solutions.

In addition, machine learning and data mining techniques are needed to detect re-occurring complex situations that might induce a security-threat to the surveillance system. Therefore, video-data from several SCs needs to be aggregated and suspicious movements (in terms of trajectories, cf. the QTrajectories project that serves as input (Jänen et al., 2012)) have to be detected. Additionally, the movements and suspicious events are categorised by a pre-trained alarm-classification system. This alarm system informs the user in case of events that have been classified as suspicious and reduces the false-alarm-rate significantly.

3. User Interface. The system is designed to be used by both professional security operators and private users. We therefore aim at developing a user interface that is easy to use but also comes with all features needed to be used in safety critical environments. The notification of users in case of alarms is an important task. We will extend our existing work as described in (Hoffmann et al., 2010) by carrying our work on the user interface design further. In (Yee et al., 2012), practical solutions are given to adapt a GUI to most effectively suite the needs of different user groups under psychological aspects. Among others, this approach may help to improve the useability and acceptance of the system.

A first draft of the GUI is depicted in Fig. 4. A web browser is used on the clients in order to display the GUI whereas the business logic is running on the server side. By offering a web application users may access the system from any location with any device available (notebook, smartphone etc.). Some functionalities of the system are described in the following on the basis of Fig. 4: A screen displaying video data is taking most of the space to the right side. On the left side, the menu is displayed that contains links in order to browse a camera network and select cameras. In order to browse historical video data, a calendar will be included (in the middle of screen). Further menus will give access to further screens. E.g. reports generated by an algorithm for people counting may be accessed. In order to administrate the system, various parameters can be adjusted. As mentioned before, a shop system will be integrated in order to sell services to the user. This services can be algorithm for analysing video data or the enhancement of the system (more cameras, storage upgrade etc.).

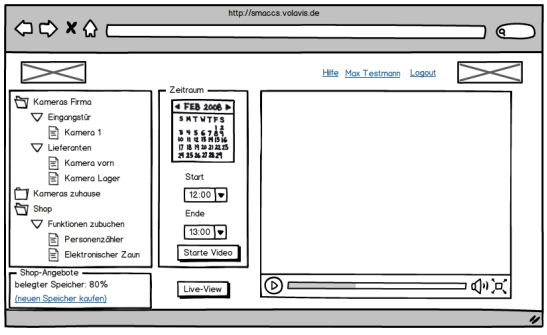

Figure 4: Possible GUI design for SmaCCS' start page.

By carefully designing the user interface we aim at reaching a broad range of users and usage scenarios that require different levels of security, privacy an the consideration of legal aspects as discussed in the following section.

4. Security and Legal Issues. The consideration of privacy is of utmost importance for social acceptance of surveillance technology. We aim at developing a trustworthy video surveillance systems by properly combining different aspects that current systems do not manage. In particular, we propose the combination of the following issues into the SMACCS framework.

First of all, we will develop a properly defined interface to detection algorithms mainly based on computer vision techniques. Thereby we make sure, the user knows exactly the data that the system generates and stores. For example, an algorithm for people counting only delivers (and stores) the number of persons moving in or out a certain area. In contrast to this, an algorithm for people detection and recognition might store data containing biometric information. By offering a well designed interface, the operators can customise the system to fit their specific needs (and laws of their respective countries (Zick, 2007)). The content protection relies not only on using convenient cryptographic techniques, but also law enforcement and user cooperation in order guarantee the legal compliance of the system. For example, we propose user pairing for accessing stored video data. In order to access data that has been saved on the system, two user have to agree on this request. After both of them logged into the system, a specified part (with time of beginning and end) of the stream is made available for viewing. Some of the ideas are based on a model for large-scale smartphone-based sensor networks that has to cope with similar challenges (Kapadia et al., 2010). In addition, the SmaCCS approach can re-use insights from the predecessor project CamInSens (Hornung and Desoi, 2011).

4 CONCLUSIONS

This paper presented a concept for a scalable and cost-efficient Intelligent Video Surveillance system for small- and medium-sized surveillance tasks, like the observation of business areas, large private households, or railway stations and airfields. The approach combines the advantages concept of Smart Cameras, i.e. cameras equipped with local processing resources, with the those of Cloud Computing, i.e. the on-demand provisioning of computing and storage services for complex calculations. Thereby, exhaustive image analysis and the management of large amounts of data, i.e. for video storage, becomes possible. The Smart Camera approach allows for the cost effective pre-processing of video data close to the sensor, while using the Cloud-concept does not require

large initial investments into expensive infrastructure components such as powerful compute servers.

Current and future work will try to find answers on the research challenges outlined in this paper. Especially, the research issues of the necessary system design, including precise system goal and system model aspects, the machine learning and efficient video/image data storage and querying are focused.

REFERENCES

Bryant, R. E., Katz, R. H., and Lazowska, E. D. (2008). Big-data computing: Creating revolutionary breakthroughs in commerce, science, and society. Computing Research Initiatives for the 21st Century. Computing Research Association.

Cernium (2013). Perceptrac System webpage. Online, http://www.cernium.com.

Chu, M., Reich, J., and Zhao, F. (2004). Distributed attention in large scale video sensor networks. *IEE Seminar Digests*, 2004:61–65.

Collins, R. T., Lipton, A. J., Fujiyoshi, H., and Kanade, T. (2001). Algorithms for cooperative multisensor surveillance. In *Surveillance, Proceedings of the IEEE*.

D'Angelo, D., Grenz, C., Kuntzsch, C., and Bogen, M. (2012). CamInSens – An Intelligent in-situ Security System for Public Spaces. In *Proceedings of the 2012 International Conference on Security & Management (SAM), 2012, 16.-19. Jul, Las Vegas, USA*. CSREA Press.

Hoffmann, M., Jänen, U., Fares, A., and Hähner, J. (2010). Amidivin: basic algorithms for alarm management in distributed vision networks. In *Proceedings of the Fourth ACM/IEEE International Conference on Distributed Smart Cameras*, ICDSC '10, pages 150–157, New York, NY, USA. ACM.

Hornung, G. and Desoi, M. (2011). Smart Cameras und automatische Verhaltensanalyse. *Kommunikation und Recht*, pages 153–158.

Jänen, U., Feuerhake, U., Klinger, T., Muhle, D., Hähner, J., Sester, M., and Heipke, C. (2012). QTrajectories: Improving the Quality of Object Tracking Using Self-Organizing Camera Networks. In *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume I-4*, pages 269 – 274.

Javed, O. and Shah, M. (2008). *Automated Multi-Camera Surveillance: Algorithms and Practice*. Springer Publishing Company, Incorporated, 1 edition.

Kapadia, A., Myers, S., Wang, X., and Fox, G. C. (2010). Secure cloud computing with brokered trusted sensor networks. In *Collaborative Technologies and Systems (CTS), 2010 International Symposium on*, pages 581–592.

Lipton, A. J., Clark, J. I., Brewer, P., Venetianer, P. L., and Chosak, A. J. (2004). Objectvideo forensics: activity-based video indexing and retrieval for physical security applications. In *Intelligent Distributed Surveilliance Systems, IEEE*, pages 56–60.

Monari, E. (2012). *Dynamische Sensorselektion zur auftragsbasierten Objektverfolgung in Kameranetzwerken*. KIT Scientific Publishing. ISBN: ISBN 978-3866447295.

Nagios Enterprises (2013). Nagios webpage. Online, http://www.nagios.org/.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In *Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09. ICSE Workshop on*, pages 44–52.

Schneiderman, R. (1975). Smart cameras clicking with electronic functions. *Electronics*, pages 74 – 81.

SML (2013). Sensor Model Language webpage. Online, http://www.opengeospatial.org.

Tomforde, S. (2012). *Runtime adaptation of technical systems: An architectural framework for self-configuration and self-improvement at runtime*. Südwestdeutscher Verlag für Hochschulschriften. ISBN: 978-3838131337.

Tomforde, S., Hurling, B., and Hähner, J. (2011). Distributed Network Protocol Parameter Adaptation in Mobile Ad-Hoc Networks. In *Informatics in Control, Automation and Robotics*, volume 89 of *LNEE*, pages 91 – 104. Springer.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. (2008). A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev.*, 39(1):50–55.

Velastin, S. and Remagnino, P. (2006). *Intelligent Distributed Video Surveillance Systems*. Professional Applications of Computing. Institution of Engineering and Technology. ISBN: 978-0863415043.

Wen, Y., Yang, X., and Xu, Y. (2010). Cloud-computing-based framework for multi-camera topology inference in smart city sensing system. In *Proceedings of the 2010 ACM multimedia workshop on Mobile cloud media computing*, MCMC '10, pages 65–70, New York, NY, USA. ACM.

Yee, C. K., Ling, C. S., Yee, W. S., and Zainon, W. (2012). Gui design based on cognitive psychology: Theoretical, empirical and practical approaches. In *Computing Technology and Information Management (ICCM), 2012 8th International Conference on*, volume 2, pages 836–841.

Zhang, L., Malki, S., and Spaanenburg, L. (2009). Intelligent camera cloud computing. In *Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on*, pages 1209–1212.

Zick, T. (2007). Clouds, Cameras, and Computers: The First Amendment and Networked Public Places. *Florida Law Review*, 69(St. John's Legal Studies Research Paper No. 06-0062):1 – 66. Available at SSRN: http://ssrn.com/abstract=956160.