Becoming a Smart City: A Textual Analysis of the US Smart City Finalists

Jasmine DeHart
School of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
dehart.jasmine@ou.edu

Oluwasijibomi Ajisegiri
School of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
oluwasijibomi.ajisegiri@ou.edu

Greg Erhardt
Department of of Civil Engineering
University of Kentucky
Lexington, KY, USA
greg.erhardt@uky.edu

Jamie Cleveland
Duke Energy One
Charlotte, NC, USA
jamie.cleveland@duke-energy.com

Corey E. Baker
Department of Computer Science
University of Kentucky
Lexington, KY, USA
baker@cs.uky.edu

Christan Grant
School of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
cgrant@ou.edu

***Abstract*—The term "smart city" is widely used, but there is no consensus on the definition. Many citizens and stakeholders are unsure about what a smart city means in their community and how it affects cost and privacy. This paper describes how city planners and companies envision a smart city using data from the 2015 Smart City Challenge. We use text analysis techniques to investigate the technology and themes necessary for creating a smart city using surveys, document similarity, cluster analysis, and topic modeling from the seven finalists from the 2015 Smart City Challenge Applicants. With this investigation, we find that smart city requests include various technologies, and the goal of smart cities is to enhance and connect the communities to improve the lives of its' citizens. On average, aspiring smart cities requested 12 new or improved technologies. We also find that two of the seven studied smart city applications center privacy in their proposals. The analysis within gives governments and citizens a common interpretation of a smart city.**

***Index Terms*—smart city; privacy; networks; text analysis.**

I. Introduction

The concept of a "smart city" has recently led people, cities, and governments to pursue idyllic improvements to municipal infrastructure. Each stakeholder may have different expectations for how their city should invest in improvements. Currently, no standard definition for a smart city exists causing variable expectations of residents, city governments, and other community stakeholders.

Citizens have an expectation of privacy, affordability [1], and timely and interactive *information* from a smart city [2]. While innovations in technology continue, citizens are critical about how unvetted smart cities can violate intrinsic rights [3]. People are inventing methods to disguise themselves from surveillance systems using fashionable masks [4]. Citizens also depend on other products to curtain themselves from other devices, such as smart speakers [5][6]. Recent studies have shown that some popular smart technologies, such as smart thermostats, may not provide stated benefits [7]. However, laws are being proposed and passed to ensure the responsibility of the city or company protects the privacy of the citizens [8][9]. Significant costs are incurred when deploying sensors equipped with 5G or WiFi connectivity due to data subscription fees [10][11]. The transformation into a smart city is expensive (e.g., between $30 Million and $40 Billion), and only a few cities are able to obtain the resources required for upgrades [1].

In this paper, we study the finalist applications from the 2015 Smart City Challenge [12] to understand what types of technologies cities requested along with the funding requirements needed to bring smart cities to fruition. Figure 1 describes the main concerns of the citizens and city governments when envisioning smart cities according to the Smart City Challenge applications.

In Section II, we describe a survey to understand the perceptions of smart cities in relation to privacy and cost. In Section III, we perform a detailed textual analysis of the submitted smart city applications. We then propose solutions to the cost and privacy issues in Section IV-A and Section IV-B, respectively. Furthermore, we describe a case study of a privacy-enabled low-cost smart city technology implemented in a U.S. city in Section IV-C. Finally, we summarize our findings in Section V.

II. Surveying perspectives of Smart Cities

We deployed a survey (IRB #13565) to learn about the current understanding of people tangentially involved with smart city implementation or governance. The survey was compromised of eighty-eight questions and had a respondent size of six participants. The average time to complete the

This material is based upon work supported by the National Science Foundation under Grant No. 1952181.

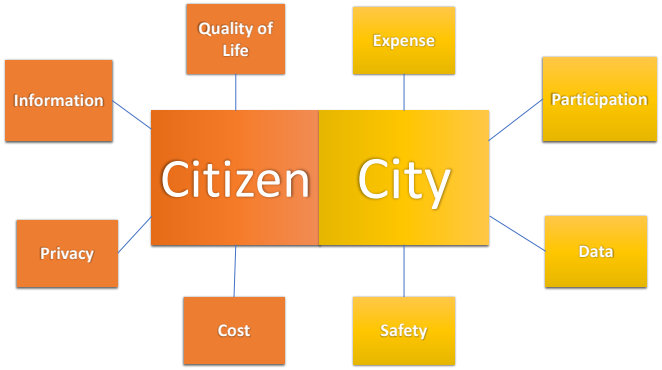

Fig. 1. Citizen and City concerns with Smart City Technology and Services. Citizens concerns centers around information, privacy, costs, and quality of life. City concerns in regards to Smart Cities focus on expenses, safety, data, and participation of the community.

survey was twenty-seven minutes. The participants were able to complete the survey online and it did not require the participants to answer every question. The survey focused on participant's knowledge of privacy, their respective government/companies' involvement with developing smart cities, and the current cost of data collection. Participants were asked about projected costs spent on technologies, knowledge of smart city efforts, and understanding of privacy expectations (see Table I).

Respondents had insightful answers when asked to define smart cities. One participant highlighted "pressing issues for its residents and businesses" and defined a smart city as:

> "One that employs technologies to improve services to the community and/or make government operations more efficient and effective. A truly smart city/community should also be targeting the most important and pressing issues for its residents and businesses not just applying technology for technology's sake." – Survey Respondent

Another respondent stated that a smart city is:

> "A city whose residents are connected by technology, high-speed broadband, providing services online and interactively, tele-health services, using IOT and AI in traffic management, air quality management, parking, waste management, public safety, utilities, autonomous vehicles, etc." – Survey Respondent

Beyond understanding what people defined as a smart city, we wanted to gain insight into the privacy concerns in potential and deployed smart cities. When asked to define privacy, participants highlighted the need to be able to revoke access to their data.

> "...I would include the ability to control or at least delete personal data as well that has been collected especially if the data has become obsolete or inaccurate." — Survey Respondent

When asked about what data privacy protection methods would help improve their willingness to take part in city data sharing, several participants stated they would like the "ability to review" any data collected by the city concerning them. If data is collected anonymously, there is an inherent difficulty when designing systems to review personalized data requests. To solve this, respondents suggest block chain or smart contract techniques to provide anonymous keys to support audit requests. Analyzing the current results, we found common concerns around the concept of privacy. The words *personal, private, uninvited surveillance and protect* are the noticeably frequent words used to describe and articulate how privacy is visualized for both pedestrians and companies. The survey further asks about data sharing. Participants were asked if they were comfortable sharing their data for the development and enhancement of smart cities. However, the results show participants are skeptical about sharing their data with smart cities. The reasons provided by the participants included possible increased policing in under-served communities, vulnerability to data leakage, and not being aware of the purpose of data collection.

TABLE I. THE SURVEY IRB #13565 WAS COMPROMISED OF MULTIPLE-CHOICE QUESTIONS AND SHORT ANSWERS. WE ADD SELECTED QUESTIONS FROM SURVEY RELATED TO DEFINING A SMART CITY, PERSPECTIVES OF PRIVACY, TECHNOLOGY, AND SPENDING.

Number	Question
1	How would you define a smart city/community?
2	How would you define privacy?
3	What data privacy protection methods would increase your willingness to share data with the city?
4	Would you be comfortable sharing personal data within these smart communities?
5	What makes you feel uncomfortable with sharing your personal data within smart communities?
6	How do you use the pedestrian counting data – for what purpose(s)?
7	How much do you spend annually on pedestrian counting data?
8	Where are the locations you need to have pedestrian counting data?

When asked about pedestrian counting for marketing and economic development, some of the pain points concerning pedestrian counting include cost and frequency of pedestrian counting, while privacy is the most valued feature with simplicity as the second most valued. According to the preliminary survey responses, companies spend between $11,000 - $20,000 annually on counting pedestrians. The average amount companies spend on data collection for traffic counts is approximately $25,000 annually; while the maximum allotted amount for traffic counting is $150,000. We also found that, although companies use pedestrian counting for marketing, economic development, safety, and infrastructure development; some of the pain points or challenges concerning pedestrian counting are cost and frequency of pedestrian counting. The most common places for pedestrian counting include intersections, downtown, or shopping areas.

III. Analyzing Smart City Finalist Applications

In 2015, the United States Department of Transportation announced the Smart City Challenge, which asked cities in the US to create an integrated, smart, and efficient transportation system built on data, applications, and technology in an effort to improve the lives of their citizens [12]. The Smart City Challenge received 78 applicants describing what a smart city looked like for their community. From this challenge, the seven cities chosen as finalist include: Columbus (Ohio), Austin (Texas), Denver (Colorado), Kansas City (Missouri), Pittsburgh (Pennsylvania), Portland (Oregon), and San Francisco (California). Figure 2 displays U.S. cities that are applicants 2015 Smart City Challenge Applicants, of these, the red circles denote the seven finalists (the circle area denotes the population size).

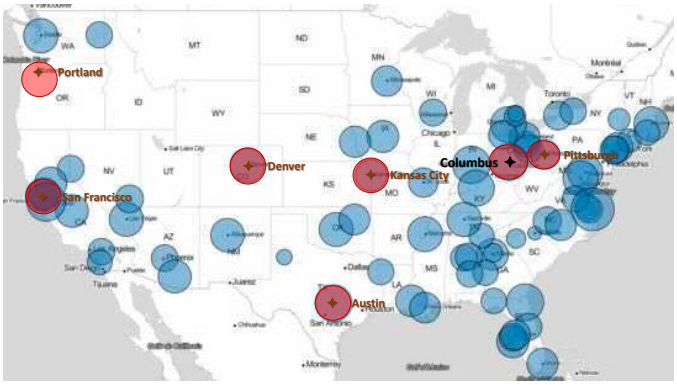

Fig. 2. Smart City Challenge Applicant locations in the United States; red circles denoted the seven finalists.

In an effort to understand the needs and wants of smart cities, we evaluate the finalist from the Smart City Challenge. We perform text analysis methods from each submitted application. We first describe the document preprocessing to transform the PDFs into a usable format (Section III-A). We then perform document similarity, where documents refer to the finalist applications, and we analyze overlap in the application requests (Section III-B). Next, we performed cluster analysis to group the finalist applications by themes according to word usage in each document (Section III-C). Additionally, we performed topic modeling to derive the dominant themes present across the documents and provide insights on what a "smart" city is compromised of (Section III-D). Furthermore, we provide details on the requested technology (Section III-E) and privacy mechanisms (Section III-F) for the Smart City Challenge finalists considered for implementation.

A. Document Preprocessing

Each finalist document was downloaded from the Smart City Challenge website where their vision statements were made publicly accessible as a PDF file [13]. We extracted the textual content from the files with Python code using the PyPDF2 PDF manipulation library [14].

Figure 3 shows the distribution of word tokens across all documents with a truncated tail. The documents are cleaned by

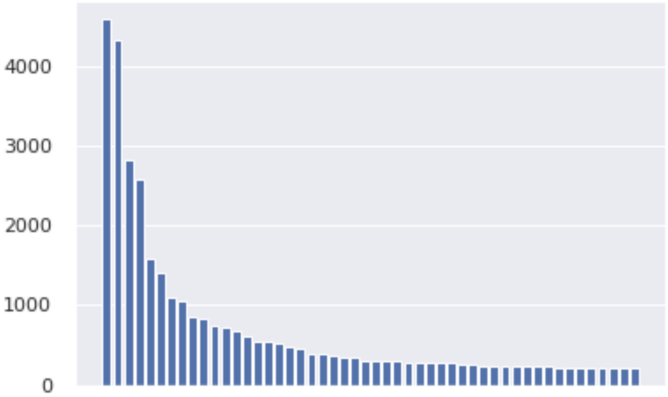

Fig. 3. Token Frequency Distribution across the Smart City Finalist Corpus. The higher frequency tokens are conjunctions and overly common words.

removing stopwords and alphanumeric text, then those words are stemmed. The words are further processed and embedded using natural language processing tools. Stopwords are derived from a list of typically infrequent words or misspellings (e.g. "asd", "buisness") or overly common words (e.g. "the", "a", "is") and overly specific city names. We calculate tf-idf scores [15] with

$$tf_{t,d} = \frac{f_{t,d}}{\sum_{t' \in d} f_{t',d}}, \quad (1)$$

where t, d are the term and document, respectively, and the ratio $f_{t,d}$ is the frequency of a term t in document d. We multiply the tf score for each term by an idf term to account for words that appear in each document. The inverse document frequency is given by

$$idf_t = \log \frac{(1+n)}{(1+df_t)} + 1, \quad (2)$$

for each term t, where n is the total number of documents, and df_t is the number of documents where t appears. We the value $tf_{t,d} * idf_t$ to remove additional terms that add little to no meaning to the content of the topics and themes. The repetition and frequency of unimportant words can influence the text analysis results.

The process of removing alphanumeric terms can alleviate typos as well as unsupportive words. Another pre-processing method we used was stemming. We used the Porter Stemmer to remove the endings of words to set them to the root [16]. When using this Stemmer, you will notice endings such as "ing", "ed", and "es" being removed. With this collection of processed documents, we create a corpus which is used in the analysis steps. With the use of Text Analysis, we can extract the text from these documents to create machine-readable information to perform machine learning tasks to better understand the content.

B. Document Similarity

With a cleaned corpus, we can gain insights of the documents by comparing them with similarity metrics. The document similarity can be calculated by comparing vectorized

documents with the Euclidean distance measure. When two documents are compared, the Euclidean distance score between them acts as a proxy for the similarity of the documents. These distances are visualized in Figure 4.

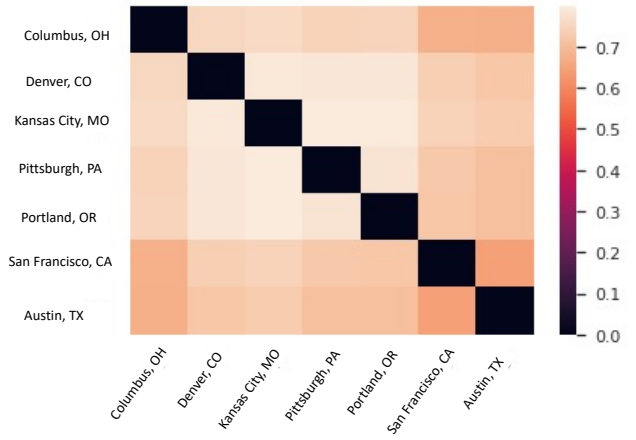

Fig. 4. Similarity Matrix for Finalist Documents; darker shades describe the similarity strength of the Smart City Finalist Applications.

Figure 4 shows relations by varying the intensity of the colors between the range of 0 to 1. The stronger correlations are noted in the darker shades with the values being closer to zero. Weak correlations are shown in the lighter shades with the values being closer to one. From Figure 4, we observe that the documents with the strongest similarity are `San Francisco`, `Columbus`, and `Austin`. The applications for the cities of `San Francisco` and `Austin` show the closest similarity among all documents. The moderate color variation across the corpus insists that the documents have similar content, but also distinctive features as shown in the additional analyses below.

C. Cluster Analysis

Cluster Analysis was performed to group similar documents together. The documents that are found in the same cluster are more similar than those in the other clusters. The cluster analysis was completed using K-Means clustering [17]. K-Means is an iterative centroid based clustering method that creates groups based on closeness or similarity. It uses expectation maximization to place the centroids at an optimal location in the data space such that similar documents are in a cluster and dissimilar documents are not clustered. For the K-Means algorithm, we must define a k value, which is the number of clusters the K-Means Model should produce. To obtain the k value, we evaluated the elbow of the corpus by fitting the model to various values of k between two and six. This elbow analysis of a corpus helped us determine the optimal number of clusters for the respective corpus [18]. The optimal k value was found when the cluster number is set at 4. The corpus was then passed into the K-Means Model to cluster the documents.

To create this visualization, we used Principal Component Analysis (PCA). PCA is traditionally used as a dimension reductionality method. We employ PCA to create a visualization that helps us understand the clusters – we choose the first two principal components as the axes of a two-dimensional plane. This cluster visualization is shown in Figure 5. From this visualization, we notice four distinctive clusters.

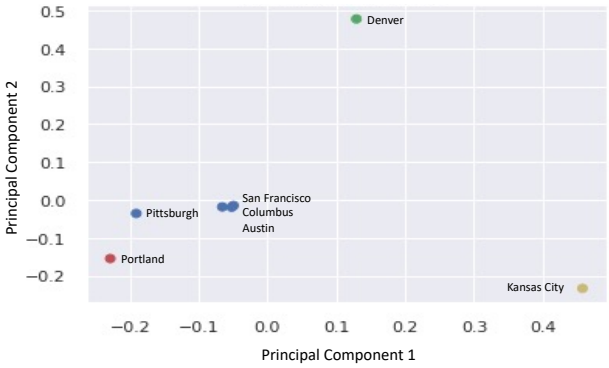

Fig. 5. Two Component PCA for visualizing K-Means Clustering for Smart City Challenge Finalists.

The cities of `Denver`, `Portland`, and `Kansas City` are individual clusters which imply that they differ from one another as well as the large cluster. The larger cluster is comprised of `Pittsburgh`, `San Francisco`, `Columbus`, and `Austin`. The content in these documents are closer in similarity. The centroid of this cluster is positioned on `Columbus`. We also see that there is heavy overlap in `San Francisco`'s and `Austin`'s applications, which are also present in the similarity matrix described in Section III-B.

D. Topic Modeling

To start the Topic Modeling process, we begin to define phrases and vocabulary from the corpus. When building the word dictionary for this model, we choose the words that appear in more than two documents but less than 90% of all documents. After this process is complete, we create a Latent Dirichlet Allocation (LDA) Topic Model [19]. LDA can produce weighted topics based on the analysis of the corpus. Our corpus consists of seven documents and a vocabulary size of 2,282. With this generative probabilistic model, we are able to derive themes and topics that are representative of the corpus. Topics are represented as a list of weighted terms of which we take the top-k. Our LDA model creates 3 topics that are used to discover themes for our documents. In Table II, the three topics are displayed with their respective words and themes.

The terms denoted in gray have little to no contribution to the theme of the cluster. These terms are used based on their assigned weight from the output values of the LDA model and the assigned topics. From Table II, we see that Topic #1 includes four cities (`Columbus, Kansas City, San Francisco, Austin`), Topic #2 includes two cities (`Denver and Pittsburgh`), and Topic #3 includes one city (`Portland`). These applications focus on several topics, but the overall similarity of the document content allowed the model to group and create topics. The documents were

TABLE II. TOPICS AND THEMES DERIVED FROM THE LDA MODEL. THE GROUPS ARE LISTED WITH ASSOCIATED CITIES, TOPICS, AND THEMES. THE TOPICS LISTED CONTAIN THE TOP TEN WORDS.

#	Cities	Topics	Theme
1	Columbus, Kansas City, San Francisco, Austin	grant, proposal, event, digital, automated, university, demonstration, automated vehicle, deploy, tool	Autonomous Technology and Tools
2	Denver, Pittsburgh	component, grant, department transportation, university, benefit, consortium, efficiency, foundation, percent, avenue	Building Partnerships and Infrastructure
3	Portland	device, efficiency, equity, percent, market place, university, cloud, engineering, payment, benefit	Connecting the Collegiate Experience to the City

assigned to these groups by their dominant topic. The themes derived from these groups encompass the various focuses a smart city can have. From these themes, it is implied that cities can become "smarter" with the use of autonomous technology, building partnerships and infrastructure, and connecting to the local universities in the city.

E. Technology Enhancements

To define the essence of a Smart City, we establish the universal technologies requested by smart cities. We introduce definitions needed to build a basis for understanding the foundation of the technologies requested by these Smart City finalists. These definitions provide a foundation to understand the types of connectivity and technology smart cities need to be operational and effective. There are additional technologies, networks, and sensors not mentioned that smart cities can implement in their community.

Many cities are interested in *Dedicated Short-Range Communications* (DSRC), which allows vehicles to communicate with each other and other road users directly. It is a wireless communication technology that can function properly without involving cellular or other infrastructures. It can save lives by cautioning drivers of a looming, threatening situation or occurrence in time to take necessary actions to help evade the situation.

Cities are also interested in technologies that improve efficiency for travelers. *Traffic Signal Priority* (TSP) can be defined as technological set of operational improvements to shorten the wait time at traffic signals for vehicles and prolong the time for green light signals. This can be done by using the existence of vehicular locations and wireless communication to extend the time of the green light at a traffic signal. TSP can be implemented at street intersections. Additionally, pedestrian counters can be implemented in these intersections as well. *Pedestrian counters* can be defined as an electronic device that is used to classify, count, and measure pedestrian traffic amongst along a particular road. These counters can be used to measure the direction of the traffic by time and location. With this technology, corporations can find peak traffic times, identify entry and exit points of travelers, and set travel management protocols. Smart kiosks can serve as a gateway for pedestrian counting as well. A *smart kiosk* is an information kiosk that detects and tracks prospective clients and sends/stores information about these prospects as data for usage [20]. These kiosks can serve as a medium among the citizens, the city, and additional technologies. *Smart parking* technologies can be defined as a strategy that infuses the use of technology to inform citizens about free and occupied parking spaces over the Web or mobile apps. Simultaneously, it can use minimal resources there by reducing time and consumption of fuel.

Electric transportation is any vehicle whose propulsion and accessory systems are powered exclusively by a zero-emissions electricity source. Electric transportation vehicles have rechargeable batteries. The E-bikes use rechargeable batteries battery mounted on the bike frame, and electric bus' battery is under the hood or protective barrier. Cities are interested in planning charging stations to support electric vehicles. Expanding from electronic transportation, smart cities are also interested in implementing autonomous vehicles.

Similarly, cities are interested in promoting *autonomous transportation*, or vehicle that drive with minimal human intervention. Also called driver-less or self-driving vehicles; autonomous transportation requires detailed real-time environmental sensing for detection and classification of surrounding objects along navigation pathways. Cities should also understand the evolving regulations of transportation governing automated vehicles. These electric and autonomous vehicles can include cars, scooters, bikes, and buses [21][22].

TABLE III. REQUESTED TECHNOLOGIES FROM SMART CITY CHALLENGE FINALIST. THE TECHNOLOGIES ARE LISTED IN DESCENDING ORDER. TECHNOLOGIES CAN BE REQUESTED BY ALL CITIES.

Technology request	**Number of Cities**
Smart Traffic Signals	7
Web Applications	7
Electric Vehicle Charging Station	7
Use of Sensors	7
Use of WiFi/Communications	7
Use of Cameras	7
Autonomous Vehicles	6
Connected Vehicles: DSRC technology	5
Smart grid	3
Use of GPS	3
Kiosks	3
Use of Cellphone signals	3
Autonomous home delivery	3
Smart Parking	3
Bike and/or pedestrian Counters	2
Electric Bus	2
Information screens for bus stops	2
Road condition monitors	2
SMART roadside lights	2
Traffic Management Centers	1
Universal smart access card	1
Bike sharing	1
Transportation Hubs	1
Interactive Voice Response	1
Smart Pedestrian Guides	1

In Table III, we display the requested technology for the cities. Among the seven finalists, 25 technologies were requested. The average city requested 12 technologies to be used in their smart city. The amount of technology requested by the city could vary depending on the population as seen in Figure 6.

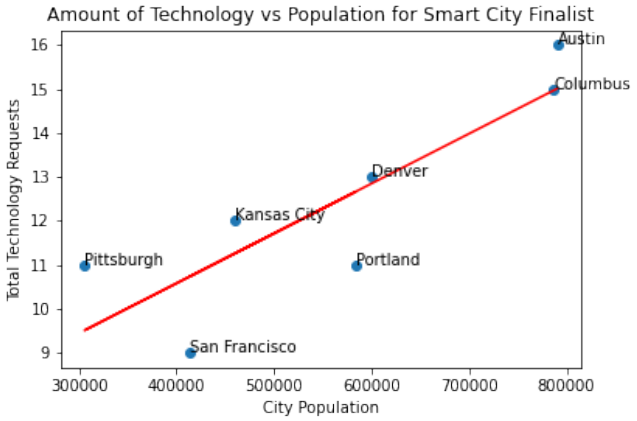

Fig. 6. Comparing the city's population size with the amount of technology requested. A linear regression line shows the projected fit for the cities.

The winning city, `Columbus (Ohio)`, requested a total of 16 technologies to implement their smart city. Following close behind is the city of `Austin, TX` with a total of 15 technology requests. The remaining cities had 13 requests (`Denver, CO`), 12 requests (`San Francisco, CA`), 11 requests (`Kansas City, MO and Pittsburgh, PA`), and 9 requests (`Portland, OR`). To integrate these technologies, the cities use sensors, video, Global Positioning Systems (GPS), and radio signals from pedestrians, vehicles, and equipment. These cities also use these video and GPS feeds for license plate recognition and to track crime-related incidents. The goal of becoming a smarter city revolves around connecting communities to opportunities, decreasing health disparities, reducing air pollution, and increasing the mobility of citizens by relieving congestion of roadways. Assisting low socioeconomic and disabled citizens has risen to the forefront of smart city development strategies. In an effort to make these advancements more inclusive of those communities, smart cities have proposed the use of:

- *Smart kiosks* enable advanced payment options by incorporating additional features, such as braille and voice feedback
- *Electronic signs* can provide visual and audio cues to pedestrians crossing intersections
- *Autonomous car sharing* allows commuters first and last mile transportation with a reduction in costs
- *Information screens* provide real-time transportation updates through audio and video

With the incorporation of these additional technologies, we see these cities becoming more inclusive and smarter for all. On top of an already costly smart city, these specialized technologies introduce additional expenses tied to continuous maintenance for supporting the aforementioned technologies.

F. Privacy Considerations in Smart Cities

A major concern for citizens in literature is understanding how increased technologies in cities will affect their privacy [3] [4][8][9]. Furthermore, cities will become a 24-hour hub for collecting information about the mobility and efficiency of transportation, but also personally identifying information of its' travellers [20]. In the Smart City Challenge [12], we examine how applicants describe risks and mitigation strategies for the deployment of technologies to their cities. From these concerns, we focus on the risks associated with residents and visitors of the city. The main concerns listed by the cities include data sharing, individual privacy, system security, data privacy, and data management.

In Table IV, we reviewed these Smart City Finalist proposals and assessed a score based on a Likert Scale (Excellent, Average, Poor) from the five central themes found in the documents: Data Sharing, Individual Privacy, System Security, Data Privacy, & Data Management. From the proposal and discussion, a city will receive a rating for all five privacy categories:

- Excellent: The proposal has thorough discussion about the risks and mitigation strategies related to topic and a solid plan of action.
- Average: The proposal has moderate to little discussion about the risks and mitigation strategies related to topic and a general plan of action.
- Poor: The proposal has little to no discussion about the risks and mitigation strategies related to topic and no plan of action.

We give each of the five categories a definition to describe their clarity of the topic in the documents. **Data management** outlines access control procedures, storage schema, and storage policies for smart city data and databases. **Data privacy** entails the encryption of items in the data, and what information is stored from the citizens and anonymization schemes. **Data sharing** includes the procedures and policies of which the smart city data will be shared with organizations, entities, or the public. **Individual privacy** focuses on the protection of citizens in the city. This protection could include, but not limited to, encryption schemes, consent documents, and privacy mitigation techniques. **System security** details the overall protection mechanisms for the smart city infrastructure.

Data sharing and data privacy concerns are addressed by the majority (4 of 7) of the cities. Strategies for addressing data sharing included access management, encryption, and anonymization. Individual privacy, system security, and data management categories are each addressed by three of the cities. Columbus is the only city without a risk analysis in their proposal. This city will develop their plan during the implementation of their city, but would this be enough? Immediately after winning, Columbus created the Smart City Program Office to assess possible risks and mitigate them. Of the finalists, none of these cities provide a detailed description

of the protection they will provide their citizens in their proposals. To mitigate the proposed risks these cities seek to: (1) implement standards from government and industry, (2) anonymize or mask sensitive personal data, and (3) partner with cyber-security experts and government.

TABLE IV. RATING OF PRIVACY DISCUSSION BY CITY. EACH CITY RECEIVES A RATING (POOR, AVERAGE, OR EXCELLENT) BASED ON FIVE CATEGORIES.

City	Data Sharing	Individual Privacy	System Security	Data Privacy	Data Management
Columbus, OH	Poor	Poor	Poor	Poor	Poor
Austin, TX	Poor	Poor	Excellent	Excellent	Excellent
Denver, CO	Poor	Poor	Poor	Average	Poor
Kansas City, MO	Poor	Average	Excellent	Poor	Poor
Pittsburgh, PA	Poor	Poor	Poor	Average	Poor
Portland, OR	Average	Poor	Poor	Average	Average
San Francisco, CA	Poor	Poor	Poor	Poor	Poor

Beyond security breaches and attacks, what protection will these cities use to ensure the privacy of those who want to remain anonymous in an "always on" city? Researchers have investigated the concerns of privacy leaks and the types of privacy leaks on social media [23]. These privacy leak concerns can be expected in a smart city where citizens are continually being monitored. To help cities protect their citizens, we propose the use of a visual mitigation library used for videos and images based on existing literature [24]. This work provides a foundation for several mitigation techniques used for social media networks; however these same technologies can be implemented to protect the citizens from surveillance concerns and privacy issues. Beyond the citizen's concern for anonymity or protection of minors, there is a concern for the type of information that is revealed in a public setting.

IV. Discussion

We provide essential interpretations and considerations for smart city infrastructure. Based on the Finalist's Applications, we propose the use of a low-cost and privacy-enabled smart city. Furthermore, we explore an existing smart city technology and provide discussion its' privacy-enabled and low-cost features.

A. Proposed Solution: Low-Cost Smart Cities

Smart City projects can be expensive to deploy and manage. Cities around the world such as San Diego, New Orleans, London, and Songdo have either proposed or invested in Smart City projects that cost between $30 Million and $40 Billion. In addition to the cost of deploying and maintaining the IoT devices themselves, a significant portion of the expense is a result of providing Internet connectivity via 5G or WiFi to those devices. These costs are a major barrier to the widespread deployment of Smart City technology and the social benefits that may ensue from that technology [25].

To alleviate the costs, opportunistic communication, such as Delay Tolerant Networks (DTNs) can be used as a backbone for Smart City communication to facilitate data that does not have real-time Quality of Service (QoS) constraints. DTNs traditionally provide opportunistic networking connections in areas with little to no infrastructure. Messages are delivered with some delay which is directly correlated with the layout, density, and mobility of nodes in the network [26][27]. Recognizing that some data are needed in real-time, edge-computing can be utilized as long as the placement of internet-connected nodes are optimized in the network. For data that can tolerate delays, the natural movement of people and vehicles through a city to transfer data between nodes. In this way, the citizens become an integral part of the smart city network itself.

In order for low-cost Smart Cities to flourish and DTNs as backbone to be practical, both the technology questions related to the devices and the network itself, as well the social aspects of how people and vehicles move through a city must be addressed. For almost 20 years there has been a substantial amount of research in opportunistic communications and delay tolerant networks; unfortunately real-world deployments traditionally fall short of their simulated counterparts [28]. Related efforts, [29][30][31][32][33][27][34][35][36], have proven the ability to deliver messages when connections are intermittent, but generally are limited to performing within simulation environments [37].

B. Proposed Solution: Privacy Mitigation Library

Cameras can be integrated into several requested technologies which makes it popular commodity. We consider how the privacy risks of cameras and video surveillance can be mitigated in smart city infrastructure. In a city where facial recognition systems are used can lead to privacy leaks due to individual privacy rights. Pedestrians carry identification, purchase items with their credit or debit cards, use physical keys to enter restricted areas, and virtual passcodes to access sensitive information. These types of sensitive content will be captured in those videos and image feeds [38][39], with the use of obfuscation we can ensure that content will not be leaked to others. Studies have shown that the use of obfuscation methods [40][41][42] can protect individual privacy. These obfuscation methods can include blurring, blocking, adversarial noise, or replacing items in visual content. Methods such as blurring and blocking alters the pixelation of the visual content to provide distortion to the human eye. These methods can be added on to objects, faces, and text in visual content. The technique of adversarial noise [43] adds a few pixels that can (1) impede a computer's ability to learn anything from the visual content even if it is in their possession, and (2) still allow the images to be visible to humans. To protect individuals identities, studies have suggested face swapping [44][45][46] which can switch detected faces of citizens with a pre-existing library of faces at their disposal.

To address this concern, we suggest the deployment of the *ViperLib*. This mitigation library will allow the Smart Cities to select from a library of mitigation techniques that can be integrated into their systems. As proposed by [24], mitigation techniques can be integrated into mobile applications, servers, IoT devices, and comprehensive systems. Techniques such as obfuscation (e.g., adversarial noise, blurring, blocking), interception, and blind vision can be integrated into this library easily ready for use. The library can also facilitate active engagement strategies for alerting authorized personnel about pertinent privacy concerns and suggesting the possible mitigation strategies for that visual content. These types of alerting strategies are similar to *Chaperone Bot or Privacy Patrol* from previous works [24]. These alerting systems can alert officials of private information that is displayed in public settings before the data is stored without additional protection. We hope that this can provide security to the data privacy and storage methods smart cities will implement. These alerting strategies are important to provide a human-in-the–the-loop system at various phases of the deployment and collection processes that these cities will have.

The *ViperLib* open-source library can be integrated into existing "off-the-shelf" packages. Citizens can select the privacy protection features that must be integrated into deployed systems. Such libraries can provide safety, security, and peace of mind to the citizens that reside in those areas.

C. Case Study: Deployed Technology in a Smart City

Smart city technology must be reliable, low-cost, and consider privacy to attract citizens to engage with those platforms. The Smart City Applications Platform (SCAP) is an example of a privacy-aware system coupled with reliable and effective management. It serves as a strong example for organizations to model pedestrian counting and computer vision technologies in smart cities. In this study, SCAP is deployed in city *C*. SCAP was created by a major utility company. This platform consists of a complete hardware and software solution which identifies various types of moving objects common to an outdoor urban environment such as bicycles, pedestrians, and scooters. At its core, SCAP is a Field Node with computer vision software that analyzes data from a high-definition camera on an edge compute device and transforms it into object count data (Figure 7A). The Field Node is available in a stand-alone enclosure or as an integrated subsystem of a digital information kiosk as seen in Figure 8. The Field Node kiosk is integrated in city *C*'s downtown infrastructure. This data can be uploaded to the Cloud (Figure 7B) as anonymized statistics after data analysis is complete (Figure 7C). The data can then be viewed in a portal or accessed via an Application Programming Interface (Figure 7D).

In order to provide data in as real-time of a manner as possible, the video analytics data is sent from the local device to the Cloud. Should the network connection be lost, data is queued in the Field Node compute device and transmitted once the network returns. This connection uses Message Queuing Telemetry Transport (MQTT) between the edge and cloud for

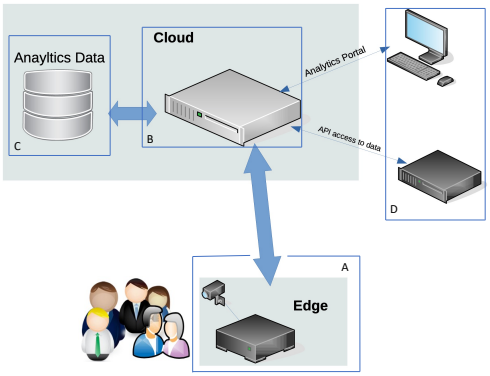

Fig. 7. High-level overview of the deployed Smart City Applications Platform (SCAP).

communication. MQTT is a standard publish and subscribe technology that uses machine-to-machine communication with low bandwidth requirements. The cloud database is set up in a cluster for backup and redundancy purposes. SCAP utilizes a cloud based user management system to control access to the Portal and to the Cloud API. In order to access any system information or data, a username and password must be created. The Platform is designed to utility-grade cybersecurity and network security standards. It is important to note that the SCAP software does not collect or record personally identifiable information, such as facial images, phone numbers or mobile phone MAC addresses. Rather anonymized target object count data is collected and provided to the user. Furthermore, all video is processed on a local computer and no images are recorded or stored ensuring piece of mind for citizens and visitors.

In consideration of robust physical security, the SCAP Field Node or digital kiosk features an enclosure with a specially keyed locking system. Both the incoming and outgoing data to the Field Node is encrypted. Through the monitoring and control software, licenses for the Field Nodes can be remote enabled or disabled. Each Field Node utilizes a compute device with storage capability. As a result, should the Field Node become compromised, the larger system is unaffected.

While the SCAP Field Nodes have the capability to work with a variety of wired and wireless data back-haul networks, the most common type is anticipated to be cellular. One of the major advantages of the SCAP is that it has low bandwidth requirements. This allows the use of the lower bandwidth CAT-M1 network when cellular communications are required. As the Smart City Applications Platform is still in its infancy and undergoing field trials, there will be ample opportunity to reduce the cost of both system deployment and operations. For example, the complexity of mounting the Field Node equipment to appropriate street furniture or buildings will be simplified and as system requirements are better understood, optimization of the Field Node components will allow for a reduction in the Bill of Material costs as well as annual operating costs.

(a) (b) (c)

Fig. 8. Field Node Designs provided by Smart City Applications Platform. (a) Field Node Integrated in a Kiosk, (b) Opened Field Node Kiosk deployed in the city, (c) Rendering of Field Node Integrated with a Light Pole (refer to Pole-Mountable Camera Support Structure, US Design Patent D902,985 S) [47]

V. Conclusion and Future Work

The finalist of the Smart City Challenge showcased what their city would look like throughout their application. We analyzed the applications to reveal the intricacies in the expectations of smart cities. When becoming a smart city, the city government and citizens could create multiple goals or milestones. From our analysis, an innovative smart city proposal would include creative approaches to deploying autonomous technology and tools such as drone delivery, building partnerships and infrastructure, and bridging the local collegiate experience in the smart city. This analysis also alluded that the typical smart city will require 12 new technologies on average to become a smart city, which is more than a city with smart technology. With creativity and development of smart city infrastructure, it is important to take cost and privacy in consideration. Using our survey and analysis, we find that privacy and cost can continue to be concerns for citizens and corporations in these environments. In the analysis of the Finalist's proposals, we find that the discussion of privacy and cost is not at the forefront of developer concerns; rather technological innovation. The winning city from the Smart City Challenge proposed innovative ways to develop their city, but showed less interest in privacy and cost than other applicants.

The analysis and evaluation of smart cities using the 2015 Smart City Challenge and deployed surveys are important to understand the needs and wants of smart cities, but also understand perspectives of individuals in those cities. These insights show the disconnect between citizens and organization who develop these smart cities. With the input of citizens for smart cities, the organizations will be able to create inclusive, adaptable and trusted relationships to aid in the acceptance and assimilation to the futuristic growth of the city.

In summary, this paper argued that smart cities have the capability to be both private and inexpensive in deployment and long-term sustainability. During planning and implementation of these cities, officials along with citizens should further consider the high cost and privacy concerns associated with their development choices. The need for privacy mitigation in smart cities extends from the protection of personally identifying information to the choice of anonymity and protect of minors. Beyond the deployment of the *ViperLib*, we proposed the use of DTNs to lower the cost of smart cities and allow citizens to assist in the transmission of data across the city. Deploying traditional IoT infrastructure is prohibitively expensive for most cities and expanded development introduces privacy risks. However, low-cost smart cities and privacy-enabled technologies can achieve the goals of smart cities while allowing citizens to feel secure and protected.

Future research considers the potential effects of security for cyber-physical systems in real IoT deployments. To do this, we will collaborate with Louisville, Kentucky, a Smart City Applicant, to discuss future strategies and deployment plans for *ViperLib* as part of NSF Grant (#1952181).

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1952181. Thank you Jason Clermont and our partners at the Louisville Downtown Partnership and Duke Energy One.

References

[1] Jasmine DeHart, Corey E Baker, and Christan Grant. Considerations for designing private and inexpensive smart cities. *The Sixteenth International Conference on Wireless and Mobile Communications*, 2020.

[2] César R Cortez and Victor M Larios. Digital interactive kiosks interfaces for the gdl smart city pilot project. 2015.

[3] Joshuas Emerson Smith. As San Diego increases use of streetlamp cameras, ACLU raises surveillance concerns, August 2019. last accessed on 09/01/2020.

[4] Adam Harvey. Cv dazzle: Camouflage from computer vision. *Technical report*, 2012.

[5] Jack Morse. There's a privacy bracelet that jams smart speakers and, hell yeah, bring it. last accessed on 09/01/2020.

[6] Yuxin Chen, Huiying Li, Shan-Yuan Teng, and Steven Nagels Zhijing Li. Wearable microphone jamming. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[7] Alec Brandon, Christopher M Clapp, John A List, Robert Metcalfe, and Michael Price. Smart tech, dumb humans: The perils of scaling household technologies. *Work*, 2021.

[8] Cory Doctorow. The case for ... cities that aren't dystopian surveillance states. *The Guardian*, January 2020. last accessed on 09/01/2020.

[9] Hannah Devlin. AI systems claiming to 'read' emotions pose discrimination risks. *The Guardian*, February 2020. last accessed on 09/01/2020.

[10] Josep Paradells, Carles Gómez, Ilker Demirkol, Joaquim Oller, and Marisa Catalan. Infrastructureless smart cities. Use cases and performance. *2014 International Conference on Smart Communications in Network Technologies, SaCoNeT 2014*, pages 1–6, 2014.

[11] Esther Max-Onakpoya, Oluwashina Madamori, Faren Grant, Robin Vanderpool, Ming-Yuan Chih, David K Ahern, Eliah Aronoll-Spencer, and Corey E Baker. Augmenting cloud connectivity with opportunistic networks for rural remote patient monitoring. In *2020 International Conference on Computing, Networking and Communications (ICNC)*, pages 920–926. IEEE, 2020.

[12] U.S. Department of Transportation. Smart city challenge, Jun 2017. last accessed on 09/01/2020.

[13] U.S. Department of Transportation. Smart city challenge vision statements, 04 2016.

[14] Mathieu Fenniak. Home page for the pypdf2 project, 12 2013.

[15] Karen Sparck Jones. A statistical interpretation of term specificity and its application in retrieval. *Journal of documentation*, 1972.

[16] Martin F Porter. An algorithm for suffix stripping. *Program*, 1980.

[17] James MacQueen. Some methods for classification and analysis of multivariate observations. In *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*, volume 1, pages 281–297. Oakland, CA, USA, 1967.

[18] Ville Satopaa, Jeannie Albrecht, David Irwin, and Barath Raghavan. Finding a" kneedle" in a haystack: Detecting knee points in system behavior. In *2011 31st International Conference on Distributed Computing Systems Workshop*, pages 166–171. IEEE, 2011.

[19] David M Blei, Andrew Y Ng, and Michael I Jordan. Latent dirichlet allocation. *The Journal of Machine Learning Research*, 3:993–1022, 2003.

[20] Ruben Sánchez-Corcuera, Adrián Nuñez-Marcos, Jesus Sesma-Solance, Aritz Bilbao-Jayo, Rubén Mulero, Unai Zulaika, Gorka Azkune, and Aitor Almeida. Smart cities survey: Technologies, application domains and challenges for the cities of the future. *International Journal of Distributed Sensor Networks*, 15(6):1550147719853984, 2019.

[21] Mojdeh Azad, Nima Hoseinzadeh, Candace Brakewood, Christopher R Cherry, and Lee D Han. Fully autonomous buses: A literature review and future research directions. *Journal of Advanced Transportation*, 2019, 2019.

[22] Mark Campbell, Magnus Egerstedt, Jonathan P How, and Richard M Murray. Autonomous driving in urban environments: approaches, lessons and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 368(1928):4649–4672, 2010.

[23] Jasmine DeHart, Makya Stell, and Christan Grant. Social media and the scourge of visual privacy. *Information*, 11(2):57, 2020.

[24] Jasmine DeHart and Christan Grant. Visual content privacy leaks on social media networks. *arXiv preprint arXiv:1806.08471*, 2018.

[25] Oluwashina Madamori, Esther Max-Onakpoya, Christan Grant, and Corey Baker. Using delay tolerant networks as a backbone for low-cost smart cities. In *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 468–471. IEEE, 2019.

[26] Ari Keränen, Jörg Ott, and Teemu Kärkkäinen. The one simulator for dtn protocol evaluation. In *Proceedings of the 2nd international conference on simulation tools and techniques*, page 55. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[27] Pan Hui, Jon Crowcroft, and Eiko Yoneki. Bubble rap: Social-based forwarding in delay-tolerant networks. *IEEE Transactions on Mobile Computing*, 10(11):1576–1589, 2011.

[28] Corey E Baker, Allen Starke, Tanisha G Hill-Jarrett, and Janise McNair. In vivo evaluation of the secure opportunistic schemes middleware using a delay tolerant social network. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 2537–2542. IEEE, 2017.

[29] Roy Cabaniss, Srinivasa S Vulli, and Sanjay Madria. Social group detection based routing in delay tolerant networks. *Wireless networks*, 19(8):1979–1993, 2013.

[30] Paolo Costa, Celicia Mascolo, Mirco Musolesi, and Gian Pietro Picco. Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 26(5):748–760, 2008.

[31] Elizabeth M Daly and Mads Haahr. Social network analysis for information flow in disconnected delay-tolerant manets. *Mobile Computing, IEEE Transactions on*, 8(5):606–621, 2009.

[32] Wang Gang, Wang Shigang, Liu Cai, and Zhang Xiaorong. Research and realization on improved manet distance broadcast algorithm based on percolation theory. In *2012 International Conference on Industrial Control and Electronics Engineering (ICICEE)*, pages 96–99. IEEE, 2012.

[33] Wei-jen Hsu, Debojyoti Dutta, and Ahmed Helmy. Csi: A paradigm for behavior-oriented profile-cast services in mobile networks. *Ad Hoc Networks*, 10(8):1586–1602, 2012.

[34] Anders Lindgren, Avri Doria, and Olov Schelen. Probabilistic routing in intermittently connected networks. In *Service Assurance with Partial and Intermittent Resources*, pages 239–254. Springer, 2004.

[35] Mirco Musolesi and Cecilia Mascolo. Car: context-aware adaptive routing for delay-tolerant mobile networks. *IEEE Transactions on Mobile Computing*, 8(2):246–260, 2009.

[36] Amit Kr Gupta, Jyotsna Kumar Mandal, and Indrajit Bhattacharya. Comparative performance analysis of dtn routing protocols in multiple post-disaster situations. In *Contemporary Advances in Innovative and Applicable Information Technology*, pages 199–209. Springer, 2019.

[37] Andreea Picu and Thrasyvoulos Spyropoulos. Dtn-meteo: Forecasting the performance of dtn protocols under heterogeneous mobility. *IEEE/ACM Transactions on Networking*, 23(2):587–602, 2014.

[38] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. Sensitive lifelogs: A privacy analysis of photos from wearable cameras. In *Proceedings of the 33rd Annual ACM conference on human factors in computing systems*, pages 1645–1648. ACM, 2015.

[39] Mohammed Korayem, Robert Templeman, Dennis Chen, David Crandall, and Apu Kapadia. Enhancing lifelogging privacy by detecting screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4309–4314. ACM, 2016.

[40] Tribhuvanesh Orekondy, Mario Fritz, and Bernt Schiele. Connecting pixels to privacy and utility: Automatic redaction of private information in images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 8466–8475, 2018.

[41] Yifang Li, Nishant Vishwamitra, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1343–1351. IEEE, 2017.

[42] Terrance Edward Boult. Pico: Privacy through invertible cryptographic obscuration. In *Computer Vision for Interactive and Intelligent Environment (CVIIE'05)*, pages 27–38. IEEE, 2005.

[43] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. Adversarial machine learning at scale. *arXiv preprint arXiv:1611.01236*, 2016.

[44] Iryna Korshunova, Wenzhe Shi, Joni Dambre, and Lucas Theis. Fast face-swap using convolutional neural networks. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 3677–3685, 2017.

[45] Bingquan Zhu, Hao Fang, Yanan Sui, and Luming Li. Deepfakes for medical video de-identification: Privacy protection and diagnostic information preservation. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pages 414–420, 2020.

[46] Sachit Mahajan, Ling-Jyh Chen, and Tzu-Chieh Tsai. Swapitup: A face swap application for privacy protection. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, pages 46–50. IEEE, 2017.

[47] James Cleveland, Gregory S Tribbe, Louis Lombardi, Gilbert DeFreitas, and Peter Henderson. Pole-mountable camera support structure, November 24 2020. US Patent App. 29/713,374.