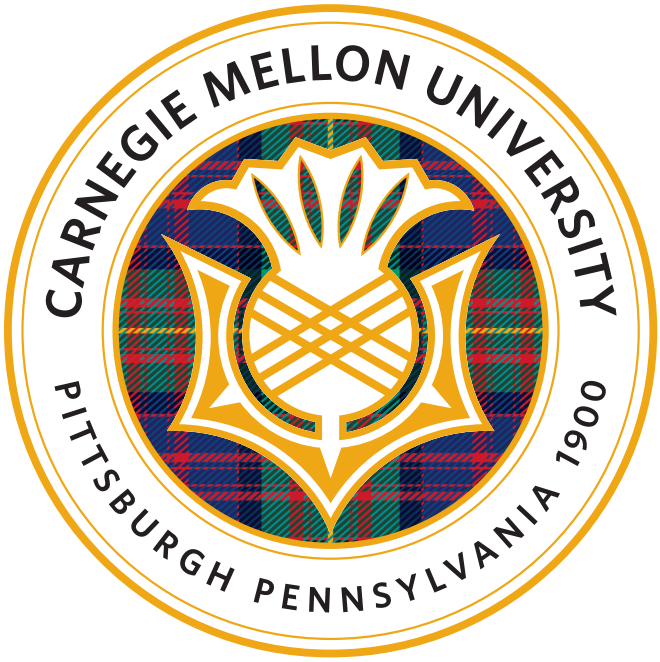
Security and Social Dimensions of City Surveillance Policy

Analysis and Recommendations for Pittsburgh



Ethics, History, and Public Policy
Senior Capstone Project
December 10, 2014

Marie Avilez
Catherine Ciriello
Christophe Combemale
Latif Elam
Michelle Kung
Emily LaRosa
Cameron Low
Madison Nagle
Rachel Ratzlaff Shriver
Colin Shaffer

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Pittsburgh currently employs numerous surveillance technologies in order to ensure public safety and is busy evaluating several others (including body cameras for police officers, drones, red light cameras, and ShotSpotter). While these tools certainly enhance the efficiency of law enforcement (or have the potential to do so in the future) there is also a risk that they can be used to infringe upon the privacy rights of innocent people. Especially as they become more pervasive and permanent, surveillance technologies may also curtail activities taking place in the public sphere—such as protests, marches and demonstrations—that are crucial to a vibrant democracy. In order to better understand this challenge, we conducted numerous interviews, case studies of comparison cities, technology reviews, as well as ethical and legal analyses of issues related to surveillance. This executive summary highlights our findings and presents our recommendations for balancing privacy and security in the context of surveillance in Pittsburgh.

ETHICAL, HISTORICAL, AND LEGAL ANALYSIS

When looking at the ethical framework for surveillance, we focused on the connection between privacy and security. For the purpose of this report, we considered privacy to be "the state of being free from outside intrusion in one's personal life" and security to be "a real or perceived safety from physical and psychological harm." Privacy is essential for self-development and individual expression and security allows the individual the basic ability to pursue personal life goals. Some surveillance measures involve a loss of privacy, and limitations must be put into place to ensure privacy rights are maintained while providing adequate security.

We believe that if a situation involves one individual's security and privacy, privacy ought to take priority. The person in question can theoretically decide what the optimal balance is between security and privacy for himself or herself. However, if a situation involves the privacy and security of multiple people, privacy can no longer be an absolute right. A claim to privacy should not allow an individual to unconditionally protect private information if this information poses a threat to the security of others.

In the case of emergency such as terrorist attacks, an initial suspension of the expectation of privacy occurs as the related level of insecurity prevents individual enjoyment of privacy's benefits. Justified surveillance can only affect those contexts that do not involve an expectation of privacy, or where a real or perceived threat negates the expectation or benefit of privacy.

Historically, surveillance in the U.S. often expands in response to periods of social turmoil and uncertainty. In addition to the surveillance of definite threats, the government has repeatedly targeted individuals and groups who question the status quo, whether or not they posed active threats to national security. It is important that we recognize that many of the rights and privileges we enjoy today are products of those who were targets of government surveillance. For example, labor groups fighting for the rights of workers in the early 1900s were excessively targeted for surveillance by the precursor of the FBI despite the fact that they were not legitimate national security threats.

During the Second Red Scare of the Cold War era, civil rights activists, most notably Martin Luther King, Jr., became targets of pervasive government surveillance, which went far beyond their public lives. As these and other systematic abuses were exposed, Senator Frank Church established a congressional committee in 1975 to investigate surveillance conducted by the intelligence community. The committee issued a scathing report in 1976, which led to the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978. This act mandated special courts to monitor the activities of the intelligence community.

While this system operated for more than a decade, the terrorist threats of the 1990s and the attacks on American soil on September 11, 2001 created a crisis that led to the dismantling of many of the controls established in 1978. In particular, the USA PATRIOT Act of 2001 provided cover for the intelligence community to expand its surveillance infrastructure. Although there have been efforts to rein in government surveillance once again, the continuing threat of terrorism has made reform difficult. This larger national conversation regarding surveillance should concern Pittsburgh for two reasons: the USA PATRIOT Act affects all levels of government. Secondly, much of surveillance infrastructure discussed in this report is federally funded.

Throughout our report, we have justified our recommendations through a holistic view of the historical, legal, and ethical frameworks surrounding surveillance and privacy.

PITTSBURGH, PENNSYLVANIA

To better understand the ecosystem of surveillance in Pittsburgh, we began by focusing technologies now in use, as well as those being considered for use. Pittsburgh has citywide CCTV surveillance systems provided by grants from the Department of Homeland Security. In 2013, Pittsburgh introduced red light cameras placed throughout the city at twenty different intersections based on the amount of traffic. The Pittsburgh Police Department is currently testing body-worn cameras.

We also examined the city's Code of Ordinances on privacy as well as community response. Unlike many cities, Pittsburgh has a privacy policy that regulates the distribution, control and transparency of public security camera systems exclusively monitoring public spaces. The purpose of the code is to prevent the potential misuse of surveillance by law enforcement and mitigate the effects of red light cameras on privacy. The Code considers cameras throughout the city to be a crime deterrent. The policy explicitly states that public security cameras can also be used for the prosecution of crimes and police have full access to the cameras. The Code targets the installation of surveillance hardware according to crime patterns. Community opinions are to be taken into account, but the Chief of Police can overrule community concerns when placing cameras in specific locations.

To protect the privacy rights of the community, the Code provides for a Public Safety Camera Review Committee comprised of government officials and supplemented by community members selected by the mayor. Additionally, public cameras must be clearly marked for areas under surveillance by public cameras. In the case of public emergencies, the police are allowed

to use these cameras in real time. The Code also provides a policy for data management. In order to formally request data, government agencies (other than the Department of Public Safety) must provide precise listing of the camera footage and submit that request for approval as part of a criminal investigation.

The Office of Municipal Investigation is responsible for enforcing this Code and the Directors of Public Safety and Information Systems are responsible for reviewing the camera system. There is a noticeable lack of obligatory statutes, with a focus on efficiency rather than privacy. Additionally, many provisions appear to be minimally implemented. Overall, the Pittsburgh Code of Ordinances provides a good base for appropriate legislation in order to balance security and privacy, but must be revised to ensure compliance and transparency.

CASE STUDIES

To better evaluate what Pittsburgh is already doing well in the context of surveillance, and how its policies and practices might be enhanced, we conducted case studies of three demographically and geographically comparable cities: Cleveland, Ohio; Minneapolis, Minnesota; and Oakland, California.

Cleveland, Ohio

In Cleveland, we focused on community response to surveillance. Cleveland currently has a variety of surveillance technologies including red light cameras, CCTV, and a Police Aviation Unit, which monitors all neighborhoods on a daily basis with helicopters. Of these technologies, the Cleveland Code of Ordinances only regulates red light cameras to prevent abuse by law enforcement. Pittsburgh's more wide-ranging code is superior in this regard.

Cleveland provides a useful case study for the analysis of the social aspects of domestic surveillance and privacy. In 2011, the Cleveland Police Department (CPD) and an independent research company conducted a Public Satisfaction Survey, surveying 375 Cleveland residents. Although there were no specific questions on surveillance, citizens of Cleveland responded that they would benefit from increased monitoring by the CPD. Generally, the survey reported high levels of satisfaction with the CPD. On December 4, 2014, however, the U.S. Department of Justice released a report highlighting systemic police brutality and excessive use force by the CPD. Clearly the extent of distrust of the CPD, especially within the African-American community, shows that the 2011 survey was flawed. However, the survey still provides a useful model for Pittsburgh to modify and implement in the future. In line with existing community engagement priorities, it is essential for Pittsburgh to gain public input when utilizing new surveillance technologies. Further, city officials must pay particular attention to the needs and concerns of the most disenfranchised and vulnerable residents of the city.

Minneapolis, Minnesota

The Minneapolis Police Department (MPD) employs various surveillance technologies, including WiFi-enabled CCTV cameras, license plate readers, squad car cameras, Taser cameras,

ShotSpotter, and mobile (trailer-mounted) cameras. The MPD owns over 250 cameras for use in the city and can access any camera, including private cameras, which have Internet access.

The City of Minneapolis does restrict the placement of cameras. There is, however, no formal requirement for the city to notify the community before installation. Most notably, neither state nor city law requires the police to notify the public of mobile cameras placed on city streets and in public spaces. Any suspicious behavior caught on camera can be used as probable cause to justify a search. At a state level, the Minnesota Data Practices Act requires that all public government information be available to the public. Individuals in Minneapolis can request a variety of data including squad car, street, and Taser camera videos. Data is deleted within three months and community members must pay a fee to access it. This policy does allow for more transparency; however, the fee may impede wide-scale evaluation of the resources by the public.

It should be noted that the public can no longer access license place reader data, after a newspaper reporter was able to track the city's mayor to a multitude of locations. After the story broke, license plate data was reclassified as private rather than public, so that only the subject can request the data. In order to achieve the appropriate level of transparency, Pittsburgh can learn from this situation, which aptly demonstrates the limits of public access to data.

Oakland, California

Oakland, California provides a useful case study for enhancing privacy and oversight provisions in Pittsburgh's Code of Ordinances. Oakland utilizes CCTV cameras, license plate readers, ShotSpotter, live traffic cameras on the freeway and street, and red light cameras. City Council proposed to combine all the surveillance into a centralized hub, the Domain Awareness Center (DAC), in an effort to upgrade the emergency operations. However, given the extent of the surveillance, the DAC could be used for many purposes other than law enforcement—e.g., to monitor groups of people as they amassed or moved through the city in an expression of democratic will. The Oakland City Council initially approved the expansion of the DAC without provisions for data retention policy or privacy policy. Public outcry stalled the expansion and forced the City Council to establish a citizen's commission to draft a model surveillance policy.

The commission based its recommendations on Seattle's well-developed surveillance code. The Seattle Code provides provisions for data management and acquisition protocols, but it lacked effective enforcement procedures. This deficiency was remedied in the draft Oakland Code. The use of Seattle's code in Oakland allows us to consider both codes as potential templates for Pittsburgh as it continues to refine its own policies and procedures. The data, operational, approval, and enforcement protocols laid out in both codes establish a clear process for the use of surveillance equipment and collected data.

INNOVATIVE TECHNOLOGIES

In addition to conducting case analysis on cities similar to Pittsburgh, we also examined innovative technologies used in other cities. New York and Chicago currently deploy red light cameras extensively and both cities have started implementation of body-worn cameras. Given the recent events in Ferguson, New York, and Cleveland, the Department of Justice has made a

push towards using body-worn cameras. Although Pittsburgh is already beginning to implement these cameras, city officials should closely watch their use in other cities in order to better recognize and address the technical and ethical challenges of this new technology.

Additionally, New York has implemented mobile observation towers, called SkyWatch, which provide the police with a better vantage point to monitor surrounding areas than they would get from ground-based observation. These towers have a potential chilling effect on public democratic participation. The NYPD maintains their cost effectiveness, but no formal research exists to assess that claim. Most importantly in support of the initiative, SkyWatch has shown a greater crime deterrent effect than traditional measures. If Pittsburgh plans to implement this technology, it should analyze New York's experience carefully. City officials must pay particular attention to the need to balance crime prevention with the potential negative impacts that such highly visible surveillance devices have on residents' sense of personal security and well-being. The impacts may be counterintuitive, especially among already marginalized populations.

Operation Virtual Shield is a joint surveillance effort between the U.S. Department of Homeland Security and the Chicago Police Department. This program has allowed the city of Chicago to network nearly 25,000 publicly and privately owned cameras spread around the city to a single emergency response center. While this closely coordinated surveillance makes it easier for Homeland Security, the police, and fire department to work together, there is little empirical evidence that it deters crime. Such coordinated surveillance projects also raise serious privacy and personal liberty issues that cannot be ignored.

The last innovative technology we examined was unmanned aerial vehicles, commonly referred to as drones. Dayton, Ohio, the home of Wright-Patterson Air Force Base and several aerospace companies, provides insight into the use of drones. Although Pittsburgh law enforcement agencies are not currently looking to implement drones in their enforcement and surveillance techniques, there is potential for such adoption in the future. Many Dayton residents have expressed alarm at the potential for law enforcement agencies to engage in persistent surveillance using drones, and there have been two high profile safety lapses involving drones in the city. Civil liberties groups, citizens, and commentators in the media have been outspoken on need for better safety protocols, and for a requirement that law enforcement agencies obtain a warrant before using drones for surveillance. They also advocate for the enactment of strong privacy policies.

In response to the situation and Dayton, and developments elsewhere, the Ohio State Legislature has developed pending legislation that will help control drone use. Among other regulations, the Senate bill, S.B. 189, and House bill, H.B. 207 provide provisions on the requirement of warrants for non-emergency drone surveillance. The bills are slightly different in the Senate and the House and both provide a useful framework for Pittsburgh to adopt at a city level in the future.

RECOMMENDATIONS

Based on our research we recommend that the Pittsburgh City Council implement the following initiatives:

- Develop and specify the parameters of "a distinct pattern of crime" needed to justify the implementation of surveillance. This can be done either within the Pittsburgh Code or as part of a law enforcement protocol related to the Privacy Code.
- Establish a more rigorous procedure for posting notices in areas subject to observation.
- Use the Oakland Code as a template for developing operational, acquisition, and enforcement protocols.
- Carry out additional research on the Seattle Surveillance Code.
- Adopt Ohio House Bill 207's language dealing with surveillance in cases of terrorist threat and adapt related provisions from Ohio State Bill 189.
- Adopt Ohio State Bill 189's oversight provisions for antiterrorist and other emergency surveillance.
- Thoroughly screen publicly accessible data to eliminate all personal identifiers from the data prior to public access.
- Consider creating a separate subsection of the Department of Innovation and Performance to conduct this screening.
- Establish a review process within the Pittsburgh Code of Ordinances for law enforcement procedures relating to surveillance.
- Task appropriate current city staff with the roles of Compliance Officer and Internal Privacy Officer. The responsibilities of these two positions are laid out in the proposed Oakland Code. In essence they will be in charge of reviewing compliance, surveillance, and enforcement protocols.
- Create guidelines for the use and evaluation of body-worn camera technology by law enforcement officials, paying close attention to privacy and data protection issues.
- Complete a Public Satisfaction and Community Response Survey with specific questions on surveillance and privacy.
- Conduct a deliberative forum prior to implementation of new surveillance technologies (including drones and Skywatch) or expansion of existing systems.

INTRODUCTION AND METHODOLOGY

Introduction

This report is the senior capstone project for the Ethics, History and Public Policy major at Carnegie Mellon University. It examines current and potential future surveillance technologies used in Pittsburgh, as well as the challenges they pose to liberty, privacy, and democratic expression. We begin by discussing the ethical and historical dimensions of security, privacy, and surveillance in a broader context. After providing an overview of the surveillance ecosystem in Pittsburgh (both in terms of technology and policy), we will present cases studies of three demographically similar cities – Minneapolis, Minnesota; Cleveland, Ohio; and Oakland, California – in order to develop a comparative understanding of the areas of surveillance policy in which Pittsburgh is already engaged and identify opportunities for city officials to learn from the efforts and experiences of other cities. We also studied other cities and communities that were not necessarily demographically comparable to Pittsburgh – New York City; Chicago; and Dayton Ohio – but provided insight into the technical, legal, social, ethical, and political dimensions of current surveillance technologies and initiatives.

We have compiled a comprehensive report that provides an overview of surveillance both in Pittsburgh itself and in our case cities, as well as the necessary ethical and legal frameworks for an effective privacy code. We conclude with a set of recommendations for sustainable and practical implementation by the City of Pittsburgh. We argue that these changes would help the city protect the rights of its citizens, while also providing public safety in an efficient and technologically advanced manner.

Origin of Project

This project emerged from a series of conversations with Pittsburgh City Council Member Dan Gilman. Our professor, Jay Aronson initially tasked us with analyzing the potential uses of unmanned aerial vehicles (drones) by city agencies, and what kinds of civil liberties issues this technology might pose for inhabitants of the city. Councilman Gilman, however, explained to us that wide-spread deployment of drones was not likely to happen in the near future in Pittsburgh or any other major American city. He noted that surveillance measures, on the other hand, were becoming ubiquitous in the United States thanks to a combination of fear of terrorism and large grants from the federal government to secure ports and major transportation thoroughfares (including rivers and bridges, both of which are a defining feature of the Pittsburgh cityscape). While Gilman assisted in the development of a comprehensive surveillance policy in the Pittsburgh Code of Ordinances as the chief of staff for former councilman (and now mayor) Bill Peduto, he felt that much more could be learned from a comprehensive study of the privacy and surveillance climate throughout the United States, and how potential technologies and safeguards for rights could be implemented in Pittsburgh. This intuition formed the basis of our research task over the course of the Fall 2014 semester.

Methodology

Once given our mandate, we began by learning as much as we could about current and potential surveillance options for Pittsburgh. We also undertook detailed analysis of relevant statutes and case law that dealt with privacy and surveillance at the local, state, and federal levels. Next, recognizing the importance of comparative analysis in developing recommendations for Pittsburgh, we selected ten cities that seemed able to provide important information and lessons for local policy. Some cities were chosen because of their demographic similarity to Pittsburgh and others for their widespread implementation of surveillance technologies over the past two decades. We ultimately narrowed our focus to three demographically and economically comparable cities and three technologically advanced cities, mentioned in the introduction. In the case of Pittsburgh and the three comparison cities, we provide the following: a description of the city and its reason for comparison to Pittsburgh, a comprehensive overview of the ecosystem of surveillance, a summary of the Code of Ordinances or surveillance policies in place, perspectives from the communities involved, and finally, a brief analysis on which we base our final recommendations. In the case of the advanced technologies possible for use in Pittsburgh, we provide a description of the current uses and analysis on effectiveness and feasibility for transfer of that technology to Pittsburgh's ecosystem.

Wherever possible, we sought interviews from local law enforcement and political officials, civil rights attorneys and organizations, and various stakeholders. We found that many law enforcement agents and city officials were reluctant to talk to us given the sensitive nature of the topic, and the political fallout resulting from the August 2014 shooting of African American teenager Michael Brown by a white police officer in Ferguson, Missouri. Fortunately, several knowledgeable people, including lawyers, civil liberties advocates, government officials, and law enforcement agents, were willing to speak with us. Unless these individuals requested anonymity, we included their views and perspectives in our report. Because of our restricted timeline, we could not engage in all of the research we would have liked to do if we had more time. As a result, many sections conclude with recommendations for follow-up research and studies. We hope that the work we have started in this project continues in the future.

TERMINOLOGY

Civil rights – Rights afforded to a citizen, which are irrevocable and inherent to participating in our society; these rights protect the individual's ability to live his or her life openly and freely.

Community – a body of people who live in the same place, usually sharing a common cultural or ethnic identity

Curtilage – the direct surrounding area of a private domicile, which extends to commercial buildings; entitled to protection as a place where occupants have a reasonable expectation to privacy which is generally accepted by the dominant society

Domestic surveillance – collection of information about the activities of private individuals/organizations by a government entity within national borders; this can be carried out by federal, state and/or local officials

Open fields – lands that are not attached to and directly associated with the home or private residence; this can be a hybrid of the private and public spheres

Privacy – the freedom to live one's life as one sees fit, with the expectation of discretion in each individual's personal life

Private sphere – the spatial and behavioral range of personal and social life; since the 1967 case *Katz v. U.S.*, the Supreme Court has recognized that the private sphere is associated with people and not just specific spaces

Public sphere – all space and life outside of that protective boundary (private sphere), subject unconditionally to government information-gathering activity

Rights – legal expectation that no entity shall infringe on one's autonomy (usually consisting of negative obligations); these are fundamental rules, obligations, and principles that govern what people are allowed to do as well as what the government is not allowed to do

Individual Security – the psychological and/or physical sense of being safe; confidence in one's safety or well-being; the state or condition of being protected from or exposed to harm

Communal or National Security – this is a focus on maintaining the survival of the state through various means such as military action, law enforcement, economic action, intelligence gathering, and political power; this is a collective protection from the dissolution of the state

Social participation - engagement with life and activities in the public sphere (extends beyond political participation)

TECHNICAL TERMINOLOGY

Body camera – A surveillance device used by law enforcement agencies to monitor interaction between police officers and citizens. It is generally mounted on the lapel or hat of the officer. The camera footage that is collected during an officer's shift is stored digitally in a database to be reviewed later by a third party.

Closed-circuit television (CCTV) – A surveillance and security system which provides remote observation of a limited area by means of one or more cameras transmitting video signals to a monitor screen/s or a hard drive, observed by a party or collected for future observation; CCTV can be used both by government agencies monitoring public spaces or by private actors monitoring their curtilage/premises

Drones/Unmanned Aerial Vehicles (UAVs) – Police departments around the country are beginning to experiment with using drone technology to aid in law enforcement. There is a wide range of the capabilities of drones including continuous video and picture surveillance. Many communities have expressed concern about the trade off between privacy and security when surveillance becomes persistent. Some communities have rejected drone use, while others have supported it.

Red light camera – A traffic enforcement camera that automatically records video and/or takes pictures when a vehicle enters an intersection after a traffic light changes from yellow to red

ShotSpotter – A proprietary surveillance system made by SST, Inc. that uses an array of acoustic sensors triggered by the sound of gunfire. These small square microphone sensors are permanently affixed to high points in a location, such as a building or street light. The sensors are set to record for a total of six seconds after the gunshot and data is analyzed in real time, triangulating, and pinpointing the location of each round fired down to the latitude and longitude.

SkyWatch – A mobile surveillance tower, manufactured by ICx Technologies, that extends 25 feet out of the top of a van. The tower can be operated by one police officer. SkyWatch can be equipped with technologies such as pan, tilt zoom cameras, spotlights, etc. This is different from average surveillance cameras because the operator can monitor a target as it moves.

Surveillance Cameras – In addition to the cameras discussed earlier, there are a variety of other cameras that can be used for surveillance. These include police car-mounted cameras and stationary surveillance cameras.

THEORETICAL, HISTORICAL, AND LEGAL ANALYSIS

This section focuses on the theoretical, historical, and legal context surrounding surveillance and privacy. It is important to have a general understanding of the ethical dimensions of privacy, in order to set limitations for surveillance as a tool for government oversight into the daily lives of individuals. Further, the history of surveillance can provide a better idea of how to move forward with surveillance since the capacity to monitor the population has grown exponentially over the last 100 years. We focused on the history of surveillance over this time period in order to more fully appreciate the surveillance boom that has occurred since the first Red Scare in the aftermath of World War I and the Russian Revolution. We demonstrate that as the technological capacity of the American surveillance state increased, so did its scale; targeted surveillance mechanisms became increasingly less discriminate, and their steadily growing complexity inhibited oversight measures. Finally, we present an analysis of the legal framework on surveillance put into place by a half century of U.S. Supreme Court rulings. Awareness of this precedent can help guide local decision making on surveillance and providing guidance on whether and how new technologies should be implemented. In our theoretical analysis, we argue that the tradeoffs between privacy and security are context-dependent. We present an ethical framework that is helpful in analyzing many different surveillance scenarios.

THEORETICAL ANALYSIS

Privacy And Security In Surveillance Context

This project document consists of extensive policy analysis and culminates in recommendations for the city of Pittsburgh's privacy code. Our analyses and recommendations are derived from an ethical analysis of two important aspects of modern life that relate to one another in complex ways: privacy and security. Our analysis will provide an ethical framework that will aid in addressing potential tradeoffs between privacy and security when making policy decisions. This section addresses the meaning and value of privacy and security and defines surveillance and its implications in relation to these. Our ethical principles for the application of surveillance derive from the examination of the tradeoffs it represents between privacy and security and the context in which these occur.

Privacy

Privacy is the state of being free from outside intrusion into one's personal life. It allows the individual to limit the access of others to his or her personal information, which consists of thoughts, speech, acts, and identifying details (e.g. medical history). Privacy fulfills two personal functions: it allows the individual to establish ownership over a conceptual or physical space in which to develop as a person, and it enables the individual to maintain or create social relationships on the basis of the admission of others into that space.

Privacy provides the framework for a personal sphere, in which the individual is free to explore his or her thoughts without intrusion from others or the fear that they should become

known. Introspection depends on the existence of such a sphere, and personal growth depends in part upon the capacity to introspect. Privacy, then, is a necessary component for self-development. Because privacy is a state free from intrusion by others, it allows the individual to control what personal information to share with others. This function is important in constructing social relationships built around tiers of intimacy. The decision to share information with one person but not others is a statement of confidence in one's relationship with that person, and it implies differential levels of trust and thereby represents an important basis for defining one's social connections.[1]

Security and Surveillance

Security involves real and perceived safety from physical and psychological harm. Actual security provides the individual with a necessary, basic capability to pursue other objectives. Perceived security facilitates processes that depend upon psychological well-being; the perception of insecurity is in itself psychologically harmful.[2]

Surveillance is the collection of personal information that an individual has not knowingly provided to the person conducting the surveillance. While we primarily are focused on state surveillance in this report, it is important to note that private entities regularly engage in surveillance as well. The typical justification for implementing surveillance is to collect the personal information of individuals who are suspected of threatening the security of others[3] to prevent or respond to a harmful action or crime. Surveillance can also serve as a deterrent to crime by increasing the likelihood of facing consequences for committing a crime.[4]

Surveillance recordings of individuals' actions can provide information that, when put together, may reveal personal information an individual would otherwise prefer to keep private.[5] Where surveillance occurs, it infringes upon an individual's privacy by removing the individual's control over the distribution of his or her personal information.[6] It provides third parties with the ability to share an individual's personal information with others, sometimes without his or her knowledge. The particular form of surveillance determines what information is recorded and, conversely, what is left within the individual's prerogative to express. Thus, surveillance has the potential to infringe on the individual privacy and the benefits it involves and requires justification when the object of surveillance has a reasonable expectation of privacy.[7]

The Relationship Between Privacy and Security

In order to assess potential tradeoffs between security and privacy, each must be conceptualized either as valuable in itself (i.e., "intrinsically valuable"), or as valuable for some other objective that it achieves (i.e., "instrumentally valuable"). Privacy is primarily instrumentally valuable in that it is necessary for individuals to achieve both self-development and autonomous relationship-building. Security, meanwhile, is both intrinsically and instrumentally valuable; insecurity is psychologically harmful, while security is a prerequisite for many valuable social processes (described later in this analysis).

Privacy and security relate to one another in two ways. First, security and privacy reinforce each other. The opportunity for self-development and introspective exploration forms part of the value of privacy, which is impaired by insecurity, perceived or actual. In the face of imminent physical danger, individuals will devote their attention to the immediate threat and in so doing cannot also apply themselves to the self-developing pursuits that privacy allows. The "unexamined life" may not be worth living on an intellectual level, but no one will stop to consider one's condition when it involves a gun to one's head.

Individuals likewise cannot enjoy the social function of privacy if they do not have the security to form relationships of any kind; the formation of civil society requires a perception of security. Imminent danger denies individuals the focus to form new or engage with existing social relationships. Circles of trust require the individual to consciously expand his or her vulnerability, a difficult proposition when under threat.

Second, security, in turn, requires privacy. Without control over one's personal information, emotional security may be compromised and physical security may be less valuable. Alternatively, privacy and security may conflict. Surveillance measures that enhance security may involve a loss of privacy. Conversely, in order to preserve privacy, limitations must exist on state surveillance and thereby on the capacity of the state to act on personal information related to security risks, such as crime.

Application of Framework

With the above framework of the relationship between privacy and security, we now move to an explication of how this framework applies to various situations.

Where one individual's security and privacy are the only factors in a situation, privacy must be paramount insofar as the individual has the capacity to use privacy to achieve other aims.[8] An individual's level of privacy varies with his or her control over the information; someone with absolute privacy could decide every article of information about him or her, which would be available to others and how others would share that information. Between this level of control to the opposite extreme, in which all information about an individual may be acquired or divulged without his or her consent (or, potentially, knowledge), there are gradations of privacy. An individual's control over his or her own personal information is essential to privacy, and the range of control described above can include the voluntary, conditional and surrender of information[9]) in the interest of personal security. In essence, the absolute protection of privacy guarantees the individual the means to optimize tradeoffs between privacy and security on his or her own criteria.

To illustrate, a person might suffer from a significant risk of heart attack or stroke. This individual could improve his or her security by submitting to the constant surveillance of a trained nurse, able to quickly respond to a health incident. In so doing, however, the individual would sacrifice a significant portion of her privacy and would no longer be able to derive many of the benefits of private life, as her most intimate sphere of life would now be subject to the constant observation of a stranger. Though an individual may be willing to sacrifice privacy for

the security of constant surveillance by a nurse, such a tradeoff should on no account be *mandatory*. The individual can best decide which he or she values more, and a baseline of privacy best allows the individual to do so by voluntarily and conditionally surrendering that privacy in increments, as he or she deems necessary.

In contexts involving the privacy and security of multiple individuals, the relationship between these two values is even more complicated. In effect, when the security of others is threatened, an individual's claim to privacy is no longer absolute. When *specific* individuals present an identified threat to the security of others, those individuals' claim to privacy is overridden by the value of the security they threaten. A claim to privacy should not protect withheld personal information necessary to state efforts to prevent or mitigate specific threats to the security of others.[10] Surveillance in this case improves the security of the threatened at the justifiable expense of privacy for the particular subjects it targets. However, this ideal depends upon perfectly substantiated confidence in the existence of a threat and the identity of its perpetrator.[11,12] Outside of the ideal case, it is uncertain who should be subject to surveillance. Therefore, individuated surveillance demands standards of precision and accountability to prevent the misuse or abuse of surveillance in response to perceived security threats.[13]

Additional cases involve individuals associated with other individuals known to threaten others. Mere association with a person threatening the security of others does not assure nor even predict complicity in the threat. However, it does place the associate on the spectrum of possible involvement, ranging from a minimum of doubtful involvement up to the maximum of complete certainty of complicity in the threat. The stronger the association between an individual and another who is known to threaten others, the more likely it is that the associate is complicit in the threat. A strong enough association provides grounds, outlined above, for prioritizing others' security over the associate's privacy, but determining the empirical threshold of strength of association exceeds the scope of this document.

In some situations it may be difficult or even impossible to determine who poses the threat *a priori*. For instance, there may be a threat to many people at one location, such as in a crowd, but it is impossible to determine which person poses the threat without the surveillance. This threat can be reduced at the expense of each person's privacy by identifying the threatening individual through surveillance. When many people are threatened, surveillance is ethically justified and therefore overrides the individual's desire not to be subject to surveillance.

The two instrumental functions that privacy performs are restricted by the state of emergency that infringe upon them. Immediate insecurity of life restricts self-development to reactionary decisions and also restricts relationship-building and social ordering through the selective distribution of exclusive personal information. When these functions are restricted by a state of emergency, surveillance cannot meaningfully infringe upon the benefits of privacy because the emergency has already completely or severely restricted them In this case, surveillance may even be helpful in regaining the former extent of the private sphere by removing the state of emergency. In cases of emergency, then, surveillance may be applied to the affected geographic areas with limited adverse effect and potentially profound benefits.[14]

However, barriers to surveillance may remain even in emergency situations. A total emergency would be one of absolute and universal insecurity, the benefits of privacy could not exist.[15] Without these, the instrumental value of privacy would be eliminated, and invasions of privacy for the purposes of restoring security become unilaterally justified up to the point where privacy again has value (i.e. where the valuable functions that privacy facilitates can occur). This point may nevertheless involve a less total form of insecurity, at a minimum either not universal or not absolute (and potentially neither). A condition of absolute but geographically localized insecurity would only eliminate the value of privacy within those localities and thereby only unconditionally justify surveillance measures in those areas. Whether universal or not, less than absolute insecurity could not justify unconditional surveillance measures; rather, it would only justify them insofar as improvements to security from surveillance would involve benefits analogous to those of privacy and greater than or equal to the benefits foregone by a loss of privacy.

Finally, surveillance may be persistent and general rather than targeted or situational. However, persistent surveillance extends far beyond an emergency context or the narrow set of individuals responsible for a security threat. Therefore, it returns to the parameters of individual privacy and security. Without an imminent threat, someone not responsible for a security threat must be able to make security and privacy tradeoffs from an initial position of expected privacy. Therefore, justified surveillance can only affect those contexts that do not involve an expectation of privacy, or where a legitimate threat negates the expectation of privacy.

The tradeoffs between privacy and security depend on the context in which these tradeoffs occur. While there are many possible scenarios, in this analysis, we have created a framework with which to categorize any situation.

HISTORICAL ANALYSIS

The most salient trends of surveillance over the past century grew out of the improvement of technology. As the sophistication of surveillance mechanisms increased, the resources necessary to monitor an individual, especially personnel, declined. Wiretaps allowed law enforcement to intercept communications from afar, and tracking devices relayed the movements of individuals without requiring someone to follow them at all times. These innovations formed new mechanisms of surveillance that increased the distance between those conducting surveillance and their subjects; establishing surveillance also became easier – a one-time wiretap replaced lengthy and sustained infiltration to capture similar information.[16]

Economies of scale appeared in the surveillance techniques of the later 20th century. Upfront infrastructural investments became the dominant costs, while maintaining surveillance over extended periods of time became increasingly efficient relative to the cost of setup; the advent of persistent surveillance through video feeds and communication taps also broadened the net that law enforcement and intelligence agents could cast. Especially in the internet age of hub-based communications, mass, even indiscriminate surveillance became not only feasible but a

resource-efficient alternative to many targeted techniques; the same suspects and any peripherally related individuals could be found and observed at very low marginal cost, and few practical disincentives remained for limiting surveillance to specific people.[17]

New instruments and their applications tested legal boundaries, as novel intrusions into the private sphere became possible and the practical barriers to established varieties of intrusion eroded until only formal legal protections remained. Often, these proved inadequate to preserve the status quo of privacy against the increasing ease of intrusion. Legislative responses and Supreme Court rulings often lagged behind the pace of innovation, as lawmakers and justices either could not fully familiarize themselves with the growing complexity of surveillance or proved unwilling to adapt their mindset from old interpretations.[18]

While the Supreme Court gradually adapted its reading of Americans' right to privacy (or right to freedom from intrusion) in the course of the 20th century and developed firmer controls on certain surveillance practices, as addressed in this report's legal theory section, a breakthrough in legislative parity with the growth of surveillance occurred in the 1970s. In the wake of the Vietnam War and the Watergate Scandal, the tarnished image of the Federal executive brought skepticism about the direction of government surveillance into alignment with political practicality and prompted the establishment of the Church Committee in 1975. Under the direction of Idaho Senator Frank Church, Congress investigated surveillance conducted by the American intelligence community and determined that a lack of oversight had allowed the widespread circumvention of citizens' privacy rights – the recommendations of the Commission emphasized active oversight rather than nominal restrictions and culminated in the Federal Intelligence Surveillance Act (FISA) of 1978, which established an explicit overseeing body of federal judges tasked with reviewing requests for surveillance authorization in cases that involved U.S. citizens.[19,20]

This period of surveillance oversight did not last indefinitely, however. After the growing fear of international and domestic terrorism in the 1990s and the paradigm-shattering events of 9/11, the PATRIOT Act renewed the freedom of the intelligence community to conduct surveillance with minimal oversight. Relatively new investigative tools such as email interception exceeded the manpower of the FISA courts, and approvals for digital surveillance greatly expanded the latitude of their recipients. The Act also provided new procedures for the rapid, almost cursory approval of more established surveillance mechanisms.[21] The controls advocated by the Church Commission and actualized by FISA were perceived as obstacles to effective counterterrorism, and these diminished or disintegrated as the post-9/11 U.S. reoriented powerfully toward security over privacy.[22]

Key Events in the History of Surveillance

This section deals with watersheds in the history of surveillance; these illustrative points chart the progression of the surveillance state from personal to impersonal and from targeted to indiscriminate – accompanying ethical analysis emphasis the ambiguities and moral abuses of those conducting surveillance, as well as the cases of legitimate surveillance that grew out of new technologies and a changing world.

Individuals who are considered heroic figures today were once perceived as threats to the nation when they were actively advocating for change. As opposition to societal norms increase, the government usually takes precautions to maintain order and security. One historical account of domestic surveillance occurred in the 1960's and involved Dr. Martin Luther King. The FBI justified continued surveillance of Martin Luther King because they were afraid that he would renounce nonviolence and join the more radical (and violent) Black Nationalist movement. The FBI began its involvement with Martin Luther King after learning that a former Communist Party "insider," Stanley Levison, was Dr. King's closest advisor, who served Martin Luther King as a ghostwriter and a financial contributor.[23] After the FBI's surveillance of Mr. Levison, the U.S. government ordered Dr. King to cut his ties with his Communist alliance. As a result of the surveillance in place, the FBI quickly knew that MLK and Levison were still in contact. Shortly after Dr. King led the March on Washington in 1963, the FBI extended its surveillance from Levison and his affiliates to King as well. The FBI set up wiretaps at King's home, offices, and hotel rooms.[24] Although they did not find any Communist activities, they did start to learn about MLK's sex life.

The FBI attempted to leak the private information that they uncovered to the press, but the stories never went too far because journalists were less willing to present details of well-known figures' personal lives than they are today. As the bureau attempted to discredit and push MLK out of his position of power through information leaks, his national influence increased.[25] In 1964, Dr. King was awarded the Nobel Peace Prize and Congress passed the Civil Rights Act. Although Dr. King did many terrific things for civil rights, the FBI continued to monitor him primarily due to an unjustified and unsupported fear that he would one day renounce non-violence and begin to foment a social revolution.

The profound intrusion into the private life of MLK is of great significance as a case application of our ethical framework for surveillance. As noted in the ethical section of this report, association with a person threatening the security of others places one on a spectrum of possible involvement in the security threat. At that point in history, communism and the growth of the Black Nationalist movement were both considered to be severe threats to national security, and MLK's connection to these radical groups was grounds to investigate his political activities. From this perspective, initial surveillance of Dr. King was appropriate, but it never uncovered adequate information to justify the egregious personal intrusion that followed.

A similar pattern can be seen in another historical example from nearly 100 years ago. As the nation entered World War I the U.S. government concentrated on eliminating threats both foreign and domestic. The Industrial Workers of the World (IWW), a labor union with radical tendencies, was known for its strategic strikes around the nation. Members of the IWW were commonly referred to as "Wobblies." The Wobblies were responsible for a wave of strikes between April and October of 1917, despite the country's involvement in World War I.[26] These strikes crippled war production and cost the industry over six million workdays. The industries most affected by these strikers were the metal trades, shipbuilding, and coal mining industries in production cities like Pittsburgh.

As members of the IWW relocated to Pittsburgh, they reached out to the People's Council of America for Peace and Democracy (PCA) to help promote IWW ideals. The People's Council was established in May 1917 and this political organization was created in opposition to the United States entering World War I. The People's Council strived to mobilize American intellectuals and workers against war efforts through a variety of public demonstrations to increase membership. During this period, the PCA's leadership vocally opposed World War I, they became a rallying destination for radicals, and they were viewed as an "umbrella organization" of the left.[27] Leaders of the IWW utilized the PCA's platform to preach their agenda of unionism.

The presence of accomplished Wobblies in Pittsburgh provided superficial evidence to claims that the IWW planned to attack steel industries. The reality though was that the IWW Pittsburgh branch struggled to secure membership and raise adequate funds for its activities. However, the federal government was secretly preparing to stop the efforts of the IWW. The Justice Department charge the IWW with preventing the war efforts and they also hoped to prove that the IWW received funding from Germans to fund their events.[28] Law enforcement received a search warrant based on the assumption that the IWW violated the Espionage Act. On September 5, 1917 local police, and U.S. Marshals raided IWW offices across the country. The raids immobilized the Pittsburgh IWW by seizing essential documents and leaving them with no funds. However, the evidence seized in Pittsburgh "contained nothing to prove that the IWW engaged in violence, treason, or had any German connection." This discovery did not stop the government's efforts to infiltrate the Wobblies, however. If anything, the lack of evidence of wrong-doing made the government look harder and even infiltrate the organization with their own operatives to extract more information and entrap key members.

The history of the Wobblies in Pittsburgh is a useful illustration of the ethical consequences of surveillance. As noted in the ethics section, surveillance may be persistent and general rather than targeted or situational. The Wobblies consistently had to defend themselves from countless instances of government harassment. From 1917 and continuing for several years, the IWW experienced targeted and persistent surveillance as a result of their radical connections with groups on the political Left. The IWW exercised their First Amendment rights, but an overzealous government agency monitored the group too heavily because they believed the Wobblies were threatening to the nation. In this case, the Pittsburgh IWW branch was raided and their privacy was invaded based on assumption rather than concrete evidence. The surveillance of the Wobblies in Pittsburgh should have stopped once federal authorities realized that they were not an imminent threat to national security.

Invasions of privacy like those experienced by Martin Luther King Jr. and the Wobblies continued unabated through the 1960s and early 1970s, prompting the Church Committee to step in to investigate these activities. In 1978 Congress passed and implemented the Foreign Intelligence Surveillance Act (FISA) to govern one especially pernicious abuse: the excessive use of wiretaps by the intelligence community. Additionally, it regulated procedures for when information that was obtained can be in criminal proceedings. The Electronic Communications

Privacy Act of 1986 also addresses wiretapping and the need to keep electronic communications private. This act limits what the government can obtain from telephone and electronics providers and what citizens can expect in terns of wiretapping and privacy in digital communication. This protects all electronic communication that is stored electronically, but excludes information that is printed.

Despite our understanding of the dangers of an unfettered surveillance state, the fear caused terrorist attacks of the 1990s (especially the first World Trade Center Bombing in 1993 and the 1995 Oklahoma City bombing) and the events of September 11, 2001 have made civil liberties less worthy of protection in the eyes of many politicians. The most expansive legislation that the U.S. government has passed on surveillance since this time is the USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). This act, passed in late October of 2001, amended FISA and provided the government additional opportunities to conduct surveillance both on U.S. citizens and non-U.S. citizens. Most notably, the sole purpose of surveillance was no longer only for foreign terrorist attacks. This was and continues to be a very controversial piece of legislation as it provided the government many more freedoms to conduct surveillance and monitor citizens. Although it did provide a caveat that citizens could not be monitored for activities protected by the First Amendment, this mandate is difficult to enforce. The act was originally to expire in 2005, but has been extended numerous times and is still in place. Many politicians on the left and the right have sought to balance these new powers with increased protections for individual liberty and privacy (including through a series of amendments to FISA in 2008 and the recently tabled USA FREEDOM Act of 2104), but the recent Edward Snowden revelations make it clear that the federal surveillance state is more powerful than ever.

In today's society, our activities are being monitored, not just by government agencies but by companies as well. In a recent opinion article, Felix Stadler argues that we are now shadowed by a "data body" that follows and precedes us, meaning that people are able to make judgments about us before they meet us, based on information that used to be considered private. Information about others provides a tool that allows people to "influence the behavior of those whose data is being held." [29] A major problem with this is that there is no way for us to know who exactly has our information. It is increasingly difficult to actually have control over our privacy. Because of technological advancements, it is nearly impossible to avoid creating personal data. Lines are not clearly drawn regarding when we do want others to be able to easily access our data, such as safety concerns. Finally, we all have different definitions of what should be considered private. We live in a society where connections are valued greatly, which makes the concept of privacy difficult to define and grasp. This brings up the importance of addressing accountability in any future policies regarding surveillance.

On April 15th, 2013 bombings at the Boston Marathon killed three people and injured many.[30] In response to this tragedy, law enforcement accessed several privately owned surveillance footage to determine who was responsible. Investigators were able to identify suspects using footage from a Lord & Taylor security camera across from the site of the

bombings.[31] This tragedy was an imminent threat to people's security. At this point, people's lives were at great risk, thus suspending their personal concerns for privacy. Boston handled the situation well, not stretching beyond rational limitations of surveillance. Boston's success with using surveillance restored security to the city, when they determined who was responsible for the tragedy. After the city of Boston solved the crime, they did not expand their surveillance methods. This is an excellent example of an ethical response to emergency circumstances without using fear as a political tactic to permanently infringe upon privacy.

In looking to create policy for Pittsburgh, it is important to have a basic understanding of the history of surveillance in the United States. It provides an important framework for understanding what has worked, what has not, the potential risks or challenges, and the difficulties surrounding government actions that are by nature, secret. Indeed, many of the concerns we face today have their origins in the long history of surveillance.

LEGAL HISTORY AND ANALYSIS

In this section we address surveillance and privacy rights and concerns from a legal perspective. Privacy rights are a major concern in today's technologically sophisticated world, where traditionally understood aspects of privacy are being eroded in the name of security. Often, these provisions of security are taken with little evidence of their efficacy, such as the widespread implementation of CCTV surveillance systems in inner cities. Since privacy rights are most often adjudicated in the U.S. Supreme Court, we will now undertake a review of the most important cases in this domain.

The Supreme Court case of *Weeks v. U.S.,* decided in 1914, began the long route to defining a person's private interests and privacy in the eyes of United States law. In *Weeks,* U.S. government officers, warrantless at the time, entered, searched and seized Weeks' "books, letters, money, papers, notes, evidences of indebtedness" in order to incriminate him.[32] The Supreme Court considered specific private interests, such as "papers" (i.e. letters sent through post, personal documents, and sealed envelopes) to fall under the Fourth Amendment. This invasion of privacy was held as unconstitutional, as the documents were seized without his presence or authority, the U.S. Marshall held no warrant for his arrest, and no warrant for the search of Weeks' premises. The decision in this matter protects the home from undue search and seizure as well as invasion by government agencies of these private interests. The concept of a warrantless search was also held as unreasonable for commercial buildings in the 1978 case of *Marshall v. Barlow's, Inc*., extending the concept beyond the private domicile.[33] The "'curtilage' of a dwelling is entitled to protection as a place where the occupants have a reasonable and legitimate expectation of privacy that society is prepared to accept."[34]

On the other hand, the case of *Oliver v. U.S.* limited the definition of curtilage and left private lands that are accessible by the public unprotected by this legitimate expectation of privacy. The Supreme Court stated: "We conclude, from the text of the Fourth Amendment … that an individual has no legitimate expectation that open fields will remain free from warrantless intrusion by government officers."[35] Indeed, this sentiment was further strengthened by the 1986

ruling in *Dow v. U.S.*[36] In this case, the EPA hired a private contractor to fly over a Dow Chemical plant and take surveillance photos of the plant complex after the company had denied an on premise search. Protocol required that the EPA go through proper channels and request a warrant; however, when the EPA disregarded protocol and used a government contractor, they circumvented what was understood by the corporation as the acceptable and legitimate recourse and violated the social contract between the U.S. government and its citizenry. This case in particular ruled that protection from unreasonable search and seizures does not apply to government officials who use airplanes to observe or photograph any land below legal airspace through which a private pilot may fly.[37] Therefore, US residents are no longer protected by the reasonable assumption that our airspace is secure from surveillance.

The legal arguments advanced in this case and others do not necessarily align completely with the ethical standards we propose for government surveillance. Whereas *Dow v. US* held that the EPA circumventing understood protocol and that targeting specific citizens or organizations through surveillance is legal, we argue that specifically targeted surveillance without a warrant of an individual unless said individual is known to be a major risk to the public safety fails to satisfy the ethical standards developed in this document.[38] Surveillance of individuals and organizations believed to pose a security risk cannot operate on any idealized certainty; we understand a certain degree of speculation goes into each instance of monitoring surveillance. We acknowledge the risk posed by some individuals to others puts the privacy of those who may cause harm to the public below the value of the security interests of potential victims of harm; however, warranting processes must be established and followed in order to preserve our ethical conclusion while preventing abusive extrapolations by those conducting CCTV and constant surveillance.[39] Warrantless invasions of privacy, which do not fall into the category of emergency justification, violate this ethical safeguard. Where these warrantless activities intrude into the private rather than public sphere, they cannot satisfy the ethical criterion for persistent surveillance and have no justification under our ethical framework.[40]

CASE STUDIES

In order to understand the strengths and limitations of Pittsburgh's current regulations on privacy and surveillance and to determine whether the city can learn from others, we decided to do case studies of comparable cities with relevant policies and surveillance technology: Cleveland, Ohio; Minneapolis, Minnesota; and Oakland, California. In each case study we provide a brief description of the city including population, size, and demographics. Further, we provide a description of the ecosystem of surveillance including surveillance technologies in use or planned for future use in those cities. We then provide an overview of the code of ordinances or governing policies relating to surveillance in those cities. Finally, when looking at potential policies for Pittsburgh, it is important to look at community response to surveillance techniques, policies, and privacy concerns to ensure avoidable concerns are addressed before potential policy implementation.

In addition to these three cities, we provide the same analysis for Pittsburgh to give a general understanding of the surveillance and policies currently in place. In the course of our research, we found that New York City and Chicago were both hubs for new and increasing surveillance techniques and technologies. Although these cities are clearly not demographically comparable to Pittsburgh, they provide an interesting look at potential technologies that Pittsburgh could be considering in the future.

PITTSBURGH

Description of City

Pittsburgh is located in the Western Pennsylvania and is the second largest city in the state, with a population of approximately 305,000 people. Spanning 58 square miles, Pittsburgh is home to many universities, companies, and industries, and is considered one of America's most livable cities. Pittsburgh's population includes approximately 66% White, 26% Black, 4% Asian, and 2% Hispanic. There are ninety neighborhoods throughout Pittsburgh with an average of 3,400 people per neighborhood. The largest neighborhood is Squirrel Hill South with over 15,000 residents. There is an average of 5,800 people per square mile with the most densely populated area in Central Oakland, where the University of Pittsburgh is situated. 5% of the population is under 5 years old, 18% between 5 and 19, 23% between 20 and 34, 33% between 35 and 59, 12% between 60 and 74, and 9% of the population over 70 years old. Over the past ten years, the population experienced a decline of about 10%. Pittsburgh has a significant amount of racial segregation with high minority populations in parts of the city such as Lawrenceville and East Liberty.

Ecosystem of Surveillance

Citywide CCTV surveillance in Pittsburgh began in 2008 as the result of a $2.6 million federal grant from the Department of Homeland Security grant for port security, with $862,000 in matching funds from the City of Pittsburgh.[41] Among the first areas targeted were The Fort Pitt, Hot Metal, Duquesne, and Sixteenth Street Bridges. However, the plan, even in the initial

stages, was to expand the network to encompass the entire downtown area, as well as other local neighborhoods. The cameras and their operators are regulated by the city's privacy ordinance adopted in 2008, which bans technology that automatically identifies or tracks persons without probable cause, and also bans operators from panning, tilting, or zooming in a way that targets an individual without reasonable suspicion of illegal acts.[42]

The installation of CCTVs in the city has grown slowly. By the end of 2008, only one of the promised twelve cameras was installed.[43] In 2009, the city received a state grant of $625,000 for tamper-proof cameras that cost more than $30,000 apiece, and in the same year, the city contracted with Aviro, a security systems company, to perform maintenance.[44] After years of working with Aviro, the city decided to invest $1 million in technology obtained through a no-bid contract with the company to implement ShotSpotter, a gunshot locator, and approximately 60 more cameras in 2013.[45] As of 2014, 153 cameras have been installed across the city in various locations. However, in spring 2014 it was reported that only 85% of these cameras were up and running due to a lack of city payments to Aviro.[46] City Council finally approved to pay Aviro for maintenance in April; the city was on track to have all cameras operational by early May 2014.[47]

In Pittsburgh, red light cameras were approved in a 7-2 vote at City Council in December 2013.[48] The placement of these cameras is just a test-run for the City to see how effective the cameras are.[49] Pittsburgh government officials decided to place the red light cameras at twenty different intersections throughout the city. The city selected these intersections because they are high volume traffic locations. The cameras will only take photos when a driver runs a red light, using vehicle make and model and license plate to identify the driver. The ordinance that allows the implementation of red light cameras in Pittsburgh must be reauthorized in 2017. By this period, Pittsburgh officials will determine whether red light cameras are benefiting the city or not.

Automated Red Light Enforcement (ARLE) is the name of the technology Pennsylvania's Department of Transportation uses to capture license plates and positions of vehicles that, intentionally or unintentionally, run red light indications. The Department of Transportation website says that the usual accidents that occur from red light runs are right-angle (T-bone) crashes.[50]

In Part III, Section 3116 E of Title 75 of the Pennsylvania DMV's Operation of Vehicles Code, it states that no automated red light enforcement system is allowed to take a front view record image of the vehicle if a violation occurs (3116.e.1).[51] There is no clear indication why this is a rule, however, it is possible that a front view image can lead authorities to falsely identify the violator since the image may not be entirely clear. This section also points out that camera equipment used for automated red light enforcement has to be incapable of "automated or user-controlled remote intersection surveillance by means of recorded video images," and information collected cannot be used for any other surveillance purposes (3116.e.2). By stating this, ARLE explicitly defines its goal to enforce violations and not to monitor its citizens' actions. The Pennsylvania Vehicle Code was modified to say that these recorded images

obtained from red light cameras have to be destroyed 30 days following the final disposition of any recorded event (3117.f.4).[52] In Pittsburgh, red light cameras will only take photos when someone runs a red light; a photo of the vehicle and license plate is used to identify the driver. The images gathered from the red light cameras are destroyed 30 days after fines are distributed. Keeping these images for more than 30 days can be a violation of citizen's privacy rights, especially since these citizens do not realize they are being photographed. They have also not explicitly stated that the government can keep these images.

In July 2013, Public Policy Polling conducted a survey of 853 Pittsburgh voters on their views towards the installation of red light cameras. A majority (59-35%) of the residents were supportive. Female participants were also more likely to support the cameras if they could be used to help catch other crimes like rapes and murders (78% of women, 51% of men, 66% of overall).[53] The option to use red light cameras to record a greater variety of incidents would not only increase the presence of surveillance in the lives of citizens but expand the availability of information in resolving crime. Though such an initiative is improbable, the statistic suggests that many Pittsburgh citizens would rather be monitored more frequently than not at all.

Despite the frequency of red light camera usage all over the country, the effectiveness of this technology is questionable. According to a driver advocacy organization called the National Motorists Association, which opposes the use red light cameras, recent installation of red light cameras all over the country has caused an overall increase in accidents at intersections.[54] The increase in accidents in intersections is a cause of people making right turns on red. When people try to make right on red, many fail to come to a complete stop; however, since drivers now have to completely stop at red lights, many cars end up in rear-end collisions.[55] Red light cameras in Pittsburgh have only been installed for about one year; however, there is no quantitative data on whether red light cameras have been successful in improving traffic safety.

Code of Ordinances and Governance

The Pittsburgh Code of Ordinances addresses surveillance policy along three dimensions of increasing precision and decreasing abstraction. Most generally, it sets rule for the distribution, control and transparency of public security camera systems installed in and exclusively monitoring public spaces. The Pittsburgh Code of Ordinances also addresses the privacy implications of red light cameras, as noted in the previous section, treating them as an enforcement mechanism rather than as an instrument of surveillance contributing and suborned to other enforcement processes. Finally, the Pittsburgh Code of Ordinances provides for the highly particular case of security surveillance in licensed garage spaces. Though less pertinent to the general issue of privacy and surveillance policy, this issue provides a potentially interesting case of limited surveillance policy in which surveillance applications are highly individuated.

The Pittsburgh Code of Ordinances expresses the "Purpose, Objectives and Principles"[56] of surveillance in terms of deterrence, comparative efficiency, and supplementation of the enforcement of criminal law.

Deterrence concerns specify "terrorist and criminal behavior" and the Code implicates these as the determinants of "strategic placement." Deterrence predominates the statement of surveillance objectives and is presented as the first order of assessment for the functionality of surveillance as an actuator of a "legitimate, clearly articulated safety purpose."[57]

This focus invokes the efficiency motive of the policy, in order to "effectively achieve their articulated purpose… more efficiently than could alternative means." The technological paradigm of efficiency pairs with "safeguards to reduce the potential for misuse and abuse of the *(surveillance)*[58] system."[59] This establishes a role for technological innovation in facilitating "administrative" solutions to policy controls on surveillance; it also suggests a tension between the efficiency of surveillance and investments in technologically facilitated accountability.

"In certain circumstances," public security cameras shall serve to provide "recorded footage in the investigation of and prosecution for criminal activity." In addition to the superseding claims of state and federal authorities on data acquired through surveillance, the Pittsburgh Code of Ordinances provides for the investigative and prosecutorial use of surveillance "footage or other data"[60] by the Department of Public Safety.[61] This provision executes the (intended) deterrent effect of surveillance through judicial avenues of criminal punishment, which operate considerably after the immediate circumstances in which a crime is committed. This differs from the possibility of police response to a crime in progress based on surveillance footage, which establishes a more immediate law enforcement presence.

Attendant to the focus of distributing surveillance technologies is the continuum between preemptive and responsive surveillance implementation. The emphasis on deterrence, coupled with the implications of the language of "strategic placement" against universal surveillance, suggests the potential viability of a predictive and thereby preemptive element in the installation of surveillance hardware. The Pittsburgh Code of Ordinances addresses and repudiates this option by requiring the identification "a distinct pattern of crime" before the installation of public security cameras, strongly orienting its explicit policy toward response.[62] The identification of deviations in crime rates is not directly addressed by the Pittsburgh Code of Ordinances. Policy or law enforcement protocol related to such determinations (e.g. what to monitor and how to aggregate and interpret incidents) may still invite preemption in the distribution of surveillance. Policy relating to the apprehension of crime according to jurisdiction may therefore be expressed at the level of surveillance strategy; their relevance to the surveillance policy depends on the invocation of "strategic" processes and can be best assessed through that connection.

The potential for protocols outside of the Pittsburgh Code of Ordinances to disrupt the privacy policy is partially mitigated by the involvement of community perspective and circumstances in the requirements for installation in the course of normal procedure. The Code requires that preliminary approval for the installation of surveillance systems must verify, under the auspices of the Chief of Police or a designee, that "the potential to deter and/or eliminate… criminal activity outweighs any concerns asserted by the affected community; there exists significant support from the affected community for the camera(s)." Discretion in assessing the crime-deterring or crime-eliminating potential in relation to the magnitude of community

concerns is reduced by a second order of approval from the Public Safety Camera Review Committee,[63] a body consisting of the Mayor, the Director of Public Safety and one other City Council member or some combination of their designees, in addition to three "members of the public appointed by the Mayor and approved by the City Council."[64,65]

Commensurately to the physical distribution of camera installations, the policy also stipulates "Notices in locations subject to the City public security cameras shall be posted stating … that such a location is subject to observation … by a public security camera system."[66] They will moreover "be directed … so that no recording is performed except of persons or events in the public right-of-way or in the public view."[67]

The regulation of the administration of surveillance considers elements practically and conceptually beyond simple controls on the distribution of camera emplacements. Circumstances of public emergency, encompassing "threat conditions connected with the safety of any person" permit the use of cameras and the footage they collect for the purpose of providing surveillance; the instability of emergencies suggests an active monitoring or virtually real-time review of recorded images and video unsuited to a lengthy approval process.[68,69]

"Law enforcement and crime prevention" also provide cause for the authorized usage of installed public camera systems; in addition to "suspected criminal activity or situations causing concerns for public safety," law enforcement may also use cameras and their footage to act on "potential for criminal activity." Active surveillance, rather than the material possibility of surveillance implied by installation, assumes a potentially preemptive quality. Greater precision in the interpretation of "concerns" and "potential" is reserved for "Department of Public Safety and/or Public Security Camera Review Committee… regulations and procedures… which shall take effect before any new cameras are active pursuant to this chapter *(Chapter 681)*"

The deterrent motive of surveillance remains expressed in the attendant discussion of "neighborhood public security cameras,"[70] but their footage "may be made available to the Police Bureau for purposes of investigating a specific crime." These installations serve an exclusively responsive purpose. It is expressly "not the intent of the City by this chapter to regulate… privately owned and operated surveillance or security cameras."[71]

The Pittsburgh Code of Ordinances also establishes a multilateral approach to the control of active surveillance and recording, combining an internal procedure of data management with a sequential protocol for the formal request of collected data by government entities "other than the Department of Public Safety."[72] The terms of authorized application from other entities stipulate "statement of the facts and circumstances surrounding the incident that has led to a request" with precise listings of the desired cameras and times; approval will only be granted in cases relating to committed, ongoing or potential crimes in which the requested footage "would provide evidence or information about the crime."

The Office of Municipal Investigations is made responsible by the Pittsburgh Code of Ordinances for enforcement of Article VIII by "Administrative Discipline" whereby "complaints

of abuse or misuse"[73] are investigated and infractions addressed by "administrative sanctions including termination."[74]

Reviews of individual public camera systems by the "Directors of Public Safety and Information Systems" will assess those systems' functionality, adherence to original purpose and community impact.[75,76]Internal regulations of the DPS determine the procedure for this review of the usage and access logs of each given system in service to the "decision to renew, cancel or alter the system."

To provide a hypothetical example of these limitations in action; a surveillance system might be installed within a particular community in response to a wave of car break-ins. After installation, the Department of Public Safety uses its operational latitude to retrieve data from cameras near the site of recent crimes. Another government entity, in order to access the same information, must request the footage for an identified purpose related to a crime. After several months, individuals become dissatisfied with the cameras after footage only tangentially related to a criminal incident is disclosed in a court case; part of the prosecution's video evidence includes footage recorded hours before the break-in, showing individuals with no stated connection to the crimes.

Community members make their complaints to the Office of Municipal Investigations, which assesses their claims. Ultimately, the Office uses its administrative authority to reprimand an employee of the DPS for abusing access to the surveillance records by including unrelated footage in the evidence. However, the Office does not apply its highest sanction - employee termination. After a further period, the Directors of Public Safety and Information Systems review the surveillance system for the community in question; they determine the surveillance achieved its original purpose of deterring crime and facilitating criminal investigation. However, continuing community concerns prompt to the Directors to alter the surveillance system by removing cameras from certain positions that generated the most criticism (such as looking into the periphery of a residential neighborhood); with these changes, the modified system is renewed.

The Pittsburgh Code of Ordinances establishes both positive authorizations of surveillance and expressly negative boundaries on the extent of those authorizations. Positive authorizations, such as the requirement of a "distinct pattern of crime" for any installation proposal, convey those phenomena which warrant the installation and administration of surveillance systems and without which surveillance must be otherwise justified, as provided by the discretionary language of the policy's Principles, or wholly removed from public administration. Within this formulation, the positive license to establish surveillance systems under particular circumstances implies the negation of such establishment under all other circumstances; the efficient statement of this positive approach can be further altered by specific prohibitions.

The motivating language of the Pittsburgh Code of Ordinances preserves discretion in the implementation of authorized surveillance by phrasing surveillance responses as optional rather than obligatory; surveillance remains an asset of deterrence and investigation rather than a

central process of law enforcement or community management. It supplements rather than drives these processes.

The Pittsburgh Code of Ordinances also extends its terms to encompass "all public security cameras… which are installed or trained on the City public right-of-way or on City property" irrespective of the origin of their funding.[77] This makes Article VIII the *superlative* policy of public surveillance in Pittsburgh, and its discretionary provisions mark the authorized avenues for surveillance innovation within the Code and the operation of the Departments of Public Safety. Its Principles and Objectives, as well as any inconsistencies thereof with other terms of the article, convey the intentions of current policy and comprise its present philosophy.

Community Response

Lawrenceville United, a grassroots organization intended to maintain the community functions of the neighborhood of Lawrenceville, has raised enough money from private investors to install sixty-two cameras of their own sixteen locations.[78] Interviews with citizens living in high-crime areas reveal a strong correlation between CCTV placement and perceived security, as well as the role fear plays in forfeiting rights for that security. Janet Gunter of Perry Hilltop Citizens Council, in the Northside, said in 2009 "'we are on the list to get at least one camera, but … when? … My neighbors are still getting shot.'"[79]

Private citizens in Southside have displayed notable support for private security cameras. New measures within the Zone 3 police department assist individual citizens in purchasing security systems. In an Oct. 2014 interview, Lt. Scirotto indicated that no citizen had expressed any concerns for their privacy rights with regards to the surveillance cameras.

While there is not a significant amount of pushback from average citizens with regards to wide spread security, civil liberties groups, most notably the American Civil Liberties Union (ACLU), do express significant concerns.. The ACLU is a non-partisan, non-profit organization that focuses on ensuring that the government does not infringe upon personal civil liberties rights. The motto that drives the ACLU activities is "Because Freedom Can't Protect Itself." Founded in 1920, the ACLU has a long history of fighting for freedom of speech, privacy, and other civil liberties. Through local chapters, the ACLU's mission is continued at the state and municipal level. The ACLU provides a variety of services to individuals including information retrieval, legal assistance, representation, and the backing of a well-known successful civil society organization. The National ACLU mainly focuses on lobbying and overall federal policies and laws that impact civil rights. The ACLU of Pittsburgh provides an expectation of privacy in all surveillance used by the government.

Analysis

We contacted city officials at many different levels of government to interview them about surveillance policy in Pittsburgh. Unfortunately, most officials were reluctant to speak to us on such a sensitive topic, and we met with resistance at many stages of the research process. This has major implications for the transparency and accessibility of surveillance information for the citizens of Pittsburgh. If citizens are unable to access information on how surveillance is

being used and what information is being gathered and shared, there is a concern about the actual use by the government. We are not suggesting that Pittsburgh makes the information gathered public, but it is important for citizens, if they make reasonable and informed requests for data and policy documents, to be provided with a general framework and process that surveillance is conducted and that information is used. This is one area in which Pittsburgh can learn form the debates that have taken place in cities on surveillance and privacy.

CLEVELAND, OHIO

Description of City

Cleveland is Ohio's second largest city with a population totaling 396,815. The city is broken down into five districts based on geographic boundaries and balanced population divisions. These districts also constitute the five police districts of the city. Each Police District has its own commander who reports to the Chief of Police for the entire city. The city is comprised on 78 square miles of land. Approximately 53% of the population is African American while 37% is Caucasian. The Hispanic and Asian populations comprise approximately 9% of the total population. Over the past few decades, Cleveland transitioned from its traditional durable goods manufacturing economy to a more service-based economy, in line with the national trend. Cleveland is generally comparable city to Pittsburgh given its size, history, economy, and demographics.

Ecosystem of Surveillance

Cleveland has implemented a variety of surveillance techniques throughout the city. One of the most important is the use of red light cameras. Currently there are 53 red light cameras stationed at important intersections throughout the city. These are the only cameras the city advertises that it uses. However, Motorola released a case study brief that outlines the introduction of video surveillance in Cleveland. The pilot program included a wireless video surveillance network from funding through Homeland Security and other federal grants. As of 2012, the report claims that there were 25 video surveillance cameras in Cleveland provided by Motorola. The Cleveland Director of Public Safety and Chief of Police are quoted praising the system. The focus of their comments is on the preventative effect the cameras have had in the city and the idea that the cameras act as a deterrent. No additional information on these cameras can be found in the public record, and these cameras do not show up in the city code of ordinances or on city websites. It is possible that these cameras are the automated red light cameras listed in the code of ordinances, however the cameras in this report have many more capabilities. We contacted Motorola for more information, however they did not respond.[80] As is the case in Pittsburgh, information on the implementation of surveillance technologies in the city is largely inaccessible to ordinary citizens. Some cities advertise their surveillance efforts, while others do not. Although there is no empirical evidence on which strategy has a greater deterrent effect, if the public does not know anything about the cameras, it is impossible for there to be a deterrent effect.

The Wireless Video Surveillance Camera System of the Public Safety Information and Technology represents the main component of increased visibility coupled with a better allocation of CPD resources, as discussed later in this section. The pilot project of this camera system in 2008 included the installation of a camera system surrounding critical infrastructure in downtown Cleveland. This was done in response to higher crime rates reported by business owners. These cameras were also placed in the vicinity of the Public Square, a major social and community area for Cleveland. Cameras are easily identifiable as they are painted black and white and display the CPD logo. In addition, flashing lights are put on top of the cameras in order to create public awareness. These cameras are also being used in the Greater Cleveland Regional Transit Authority's Multi-Agency Accessible Security Camera System. Since 2011, 32 cameras have been installed along the Euclid Corridor, a major public transportation mode for many Clevelanders and visitors. These cameras are also visible and can be monitored by CPD, State Police, Case Western University Police, and many other Police units with authority along this route. The major take away from this system is the large degree of visibility these cameras bring not only to monitoring crime but also to public awareness. This information was made available through the report while these cameras are also widely visible to the public in real life. This meets one of the general areas of improvement concluded in the Satisfaction Report. Unfortunately at this time, no information is available regarding the success rate in deterring crime through this system.

Important conclusions can still be drawn despite not having information on success rates: in applying this to Pittsburgh, visibility and information are major areas to consider. Furthermore, it appears that the use of cameras in Cleveland has a primary focus of crime deterrence rather than investigation. While the data being captured can be used as evidence in court, there is an extensive process in place to request access to this data. Regardless of what surveillance systems are implemented or what the motivations are behind the systems, there will be an even greater amount of public discontent if they are not informed.

A final mode of surveillance within the Division of Police is the Police Aviation Unit. This unit is used to increase neighborhood surveillance on a daily basis through helicopters flying over each district. There is no information regarding the exact time schedule, but CPD believed the reintroduction of this unit in 2011 after its removal for the previous five years makes better use of CPD staff and resources by being able to increase surveillance and respond to crime, the primary concern of the Satisfaction Survey.

City Ordinances and Governance

Cleveland's Code of Ordinances, specifically Chapter 237.03, Chapter 413.031, and Chapter 443.051 discuss video surveillance in a variety of ways. These are the only parts of the city code that deals with surveillance. Chapter 237.03 mandates that owners of Adult Video Arcades and Adult Live Entertainment Arcades have video surveillance in the store as well as in any viewing booths. The video cameras must be working at all times and signs must be posted letting customers know that their actions are being recorded. Additionally, the ordinance mandates that customers' bodies, from knees to shoulders, must be in view of the cameras at all

times. Storeowners are required to maintain footage for at least a week. Although this is not strictly relevant to government cameras in public places, this in an important instance of government regulating private surveillance. There are obvious reasons for a government official to support monitoring of these establishments, however a person's expectation of privacy might be different in a situation such as this. [81] Chapter 443.051 explains the different requirements of taxicab drivers in Cleveland. Each taxicab must have a safety partition, surveillance camera, or a safe. It is up to the driver/company to determine which one to use.[82]

Chapter 413.031 outlines Cleveland's policies for automated red light and traffic cameras. The cameras are deployed to catch red light and speeding violations. Fines and tickets are issued to the owner of the car or person driving the car for failure "to stop at a traffic signal displaying a steady red light" or for failing "to comply with a speed limit."[83] The ordinance clearly explains that a camera caught violation is not an actual ticket until a professional reviews it. Although the policy does not state specifically why this is the case, but we believe this is to ensure that a picture being taken by the red light camera is not automatically a ticket. For example, it is not illegal for a ambulance to go through a red light or for a funeral procession, but the camera would still flag it as a violation. A professional would understand that this is not an actual violation and ensure that a ticket is not issued.

The placement of the cameras are selected by sound professional traffic engineers and law enforcement and cameras are not permitted to be placed in a place where the "speed restrictions or the timing of the traffic signal fail to conform to sound professional traffic engineering principles." The ordinance lists all the locations of the automated traffic cameras (currently 53 locations). While the ordinance does not require that locations be listed, upon selection of new locations, the public must be made aware of those locations. Upon selection of additional cameras and before operation, the Director of Public Safety must notify the public at least 30 days before the camera becomes fully operational and can be used to ticket drivers.

Additionally, there must be a two-week period (can be part of the 30 day time period) where the violations are only considered to be warnings. Every place there is a camera, there must be a sign posted by the Director of Public Works and mobile speed units on plainly marked vehicles. Each potential ticket identified by the traffic cameras must be reviewed by a Cleveland police officer, provided in writing to the owner of the car, and the appeals process must be clearly delineated.[84] Although no explanation is given as to why this is the case, we propose that it is to ensure transparency with the public on the potential surveillance techniques used by police.

Cleveland does not regulate anything further per their code of ordinances and governing structure. In order to further understand the government oversight of surveillance techniques, we initiated a public records request with the city government of Cleveland. Although the request was received, we did not receive any further information. Given this, Cleveland has an interesting policy structure that seems to provide for transparency with red light cameras, but not with other surveillance technologies. Pittsburgh does regulate red light cameras, but Pittsburgh does not regulate other surveillance to the extent that Cleveland does.

Community Response

One of the focus areas of this research project is the social aspects of domestic surveillance and privacy, including the overall relationship between law enforcement officials who are controlling surveillance programs and the citizens of the city. There must be some balance of trust and satisfaction between these two groups because without these, it is not possible to have any sort of discussion regarding the implementation of more surveillance, let alone taking action. Surveillance requires trust because citizens are putting their faith in these law enforcement officials to better protect them and if citizens believe the surveillance is being used in a negative light, there is clearly a lack of satisfaction. A practical way to determine the level of satisfaction and trust the citizens of a city possess in their law enforcement officials is through public surveys. The survey instrument should be designed to query citizen satisfaction, feeling of citizen safety, and opinion on the future of public safety. The following is information regarding such a survey conducted in Cleveland accompanied with analysis and recommendations for how such a survey could be implemented in Pittsburgh, specifically in the context of surveillance.

The City of Cleveland Police Department (CPD), in conjunction with WPA Survey and Research, conducted a Public Satisfaction Survey in 2011 with the purpose of identifying the general levels of satisfaction of Cleveland residents with the CPD and the overall level of safeness felt within the Cleveland community. 375 respondents were used for this survey, all of which were adults. These adults were from all 5 districts of the city of Cleveland with a diversity of economic backgrounds, demographics, age, gender, and education. Grouping the survey categories of crime/violence with safety, approximately 42% of those subject to surveillance believed the most important issues CPD dealt with were public safety and protection. In response to the survey, the City of Cleveland Mayor's office finalized the Future of Public Safety Document in 2011 to better serve the citizens of Cleveland. While no specific questions regarding camera surveillance, the prevailing trend was that citizens of Cleveland believed they would benefit from increased monitoring.

When discussing the images of police leaders, police department as a whole, the satisfaction of the police department, etc., the percentage of favorability versus unfavorability was broken down into multiple levels. On average, there was a reported 67% satisfaction with the overall work done by the police department. Should a law enforcement agency wish to change policies or implement increases in surveillance, it is crucial for citizens to have a high level of trust in their law enforcement. To further the satisfaction aspect of the survey, each district of Cleveland was polled within the overall satisfaction. Lastly, respondents were asked to respond about the "courteousness" and approachability of the CPD Officers and Employees, respondents reported an 83% rate of them being "totally pleasant" in interactions with the public.

However, this particular report doesn't specify what exactly it means to be "satisfied," nor does it discuss the potential past interactions of these respondents with CPD or any type of law enforcement. Along a similar vein, 61% of respondents stated they were unfamiliar with how CPD uses its resources, where they come from, and how they allocate their staff. This is

information that should be readily available to the public for an even more transparent relationship than seems to be in existence. With respect to this issue, as of 2011, CPD has not published any new information regarding potential solutions to providing this information, but has put in many new measures and surveillance practices to increase transparency and visibility of CPD in the community such as the Wireless Video surveillance Camera System. These facts demonstrate the importance of clarity when surveying citizens to not only achieve accurate results, but to better understand where the shortcomings in communication exist and where the relationship between these groups is strongest. Furthermore, citizens become less trustworthy in their law enforcement if they aren't entirely sure where the resources of the department are going. If citizens are less informed, they are less willing to follow their law enforcement leaders thereby hurting the citizen to law enforcement dynamic. This could affect the future of domestic surveillance in a city should additions be made and should citizens continue to be uninformed. With policies surrounding surveillance, it's even more critical to inform citizens since this relates directly to individual rights. Without citizen knowledge, there would be backlash and discontent, causing more problems than solving them.

Surveillance camera projects are discussed in each of the following "umbrella groups" of Cleveland's Future of Public Safety Report: Office of Professional Standards (OPS), Division of Corrections, and Public Safety Information and Technology. A report such as this provides insight into what the city has done thus far with regards to surveillance for/with its citizens while providing detailed information on surveillance plans for the future.

With regards to OPS and the Division of Corrections, numerous surveillance cameras serve to assist in monitoring interactions between citizens and CPD in police stations within each district and within the penitentiary. These systems use surveillance to help minimize issues in the workplace, increase safety for police officers, and to theoretically to minimize the amount of police officers needed in the buildings for monitoring and patrolling, so they can be out patrolling neighborhoods and their respective districts, thus allocating resources more efficiently. The important takeaway from the report is that CPD controls the data storage and video surveillance of City Jail and OPS through the use of remotely operated cameras. As mentioned above, the idea behind these is to better position police officers out in the community or manning the camera feeds rather than inefficiently staying in their buildings. In terms of storage with these particular cameras, CPD is responsible for storing the data, but they do not disclose their method or other details with respect to these particular feeds.

There were many significant, interesting trends identified in the Satisfaction Survey. 56% of "business owners" were dissatisfied with the CPD according to the survey. In response to this, CPD began working with City Council to implement a Wireless Video Surveillance Camera System to install a pilot system of five wireless relays connected with nine cameras surrounding "critical infrastructure in downtown Cleveland."[85] The goal of this system is to support and develop effective preventative and protective measures to deter crime. While this project began in 2008, it significantly expanded in 2011 to reach a total of 19 total cameras and five wireless relays which are directed to the Office of Emergency Management where the data is recorded

and stored for up to 30 days. This office is not directly related to CPD, but rather has a larger function of protecting Clevelanders and visitors from natural disasters or terror attacks, thus making it part of the Department of Homeland Security. It is interesting that a major surveillance/public safety initiative like this is taken out of the hands of CPD, but it makes sense that Homeland Security is controlling the feed. However, CPD Downtown Services Unit has the ability to also monitor the feeds. This ability stems from a partnership between Homeland Security and the various law enforcement offices throughout the country, not only Cleveland, to promote a safer country from terror. It would follow that Pittsburgh would have a relationship with Homeland Security should its efforts with domestic surveillance come to fruition.

A second interesting trend dealt with the methodology of asking questions regarding crime and the responses. The survey structured questions on crime as whether or not it was a CPD issue or a total community issue. Between 61-69% of respondents stated it was a community issue, not one for which the CPD is solely responsible[86]. There is some ambiguity here because nothing is mentioned about what exactly the community could/should do. The only mentioned societal tool to help police is called Crimestoppers, which is an anonymous tip line that offers cash rewards for information about crimes. This is not exactly "camera" surveillance, but it is a form of human surveillance that the city uses to help deter crime. There is no information reported about the correlation between the amount of crime reported/taking place before or after the implementation of Crimestoppers. To put this system in a different light, there could be a motive of investigating crime, but that did not come through in the reports compiled.

When dealing with neighborhood safety, 84% "totally agreed" that they feel safe in their own neighborhood during the day and 63% feel safe in their own neighborhood at night. In both instances, the strongest dissenting group was the age group 18-24. When dealing with other neighborhoods, 73% "totally agreed" that they feel safe in other neighborhoods during the day while only 40% stated they felt safe in other neighborhoods at night. The strongest dissenting groups were from a particular district and from the number of respondents who were from the economic background earning less than $50k/year[87]. Again, there is incomplete information on the respondents from this district, (same with the other districts) as well as those earning less than $50k/year. There may be some overlap in this group and there may be non-statistically significant numbers associated with these groups meaning the pool of respondents that fit these particular groups could be underrepresented. While Cleveland's survey had its defects in terms of clarity, we argue that it lays a solid foundation for Pittsburgh to build on with the hope of better understanding the relationship between city residents and law enforcement so that it can create sound guidelines for surveillance technologies and practices.

Analysis

In terms of lessons learned, Cleveland has a transparent red light camera system policy that might be useful to Pittsburgh. The requirement of telling the public where the cameras are can help ensure the cameras are actual deterrents rather than retrospective crime catchers. However, the argument made by Cleveland government that the cameras deter crime is problematic given the lack of public knowledge of cameras other than red light cameras. Indeed,

the recent release of surveillance video footage showing Cleveland police officers shooting to death a 12-year old boy with a toy pistol suggests that cameras are more likely to record tragic events than to manage or prevent them.[88] This is definitely something Pittsburgh can learn. If the main focus is to deter crime when using video surveillance, the public should be made aware of the locations either through signs or distributions of their locations. In addition to this, Cleveland clearly has a lack of city code regarding the governance of cameras other than red light cameras. Pittsburgh must be aware that transparency with the public should be codified in governance with a clear oversight structure.

Prior to making recommendations regarding a Community Response Survey for the city of Pittsburgh, we conducted research to determine if any public response was already in existence regarding surveillance. According to Pittsburgh polling data, the only surveillance information the Pittsburgh community at large had responded to dealt with the use of red light cameras. According to the response, citizens believed these cameras were a positive force on their community. Furthermore, citizens stated they would be more satisfied if these cameras were used for other sources as well. This information demonstrates a community that sees the value of technology and increased surveillance. Additionally, it reveals a community that values crime prevention and crime deterrence. With a desire for increased surveillance, this infers that the discussion on increased surveillance is one the community is ready to engage in.

Within the cities used as case studies, there were key facts to take into consideration with regards to the constantly evolving relationship between the general public and law enforcement. In cities with more advanced surveillance technology such as New York, Chicago, and Oakland, law enforcement takes a reactionary approach to crime deterrence and crime prevention using the crime itself as leverage to institute new surveillance policies, thereby creating less dialogue between their respective police departments and their citizens. The Urban Institute Justice Policy Center in Chicago discovered a lack of citizen inclusion in planning systems and community knowledge, which led to a higher rate of dissatisfaction of law enforcement by their citizens[89]. Similarly in Oakland, Citizens Community was created by citizens to generate their voice in policy as a response to not knowing about surveillance policy expansion[90]. The creation of citizen organized groups signifies the importance of having open communication between the general population and law enforcement groups because without this communication, people believe their rights and right to privacy are being violated more so than if they are informed. In larger cities such as New York and Chicago, it is more challenging to create an open dialogue with the population because there are so many people. For this reason, these cities have taken a reactionary stance as the best way to minimize public dissatisfaction. If these cities were to install policies for crime prevention prematurely, there would be an even greater outrage from a larger mass of the population saying their rights are being infringed upon. However, by reacting to crime and putting into place policy measures after crime, they have a justified system where the public cannot negatively react to the same extent. Given the facts of these particular cities and their community relationships, we do not suggest Pittsburgh take a reactionary approach with its citizens.

Based on these trends, we recommend that City Council consider two major ideas when preparing to discuss domestic surveillance with the Pittsburgh population: 1) A reactionary policy makes sense, but it should be reactionary to citizens' opinions and not solely crime. There needs to be balance between reacting to crime prevention, crime deterrence, and public opinion. 2) Community involvement and community knowledge are crucial aspects for community response. Even if the community will not directly contribute to the policy on surveillance, the more they are in the know, the more they will be able to support the programs in place and support the Pittsburgh Police in their efforts.

Before moving forward with specific survey suggestions, there are two potential issues that could arise from the use of such a survey. First, the potential outcry of "racial profiling" is likely if a survey is only given in certain areas and the results unfavorably shed light on a particular group of people. Second, there is a realistic possibility that there will not be an "adequate" response by the citizens, meaning participation numbers may be low. Both of these potential issues will never be completely solved. However, there are ways to help minimize their negative effects while still giving full disclosure to citizens. The most important elements, as already discussed, are knowledge and community involvement. No matter how the survey is distributed, there should be a statement accompanied by it stating the purpose, potential future plan, where else this survey is being used, and that this is part of an open dialogue with Pittsburgh citizens. By doing this, citizens will not be justified in responding negatively in the future about not being represented or not being given a fair opportunity to contribute toward their city.

In terms of how to distribute the survey, this becomes more challenging. While in Cleveland the survey was done over the phone, this did not maximize its potential because it left out the chance for free responses from citizens thereby taking out a more inclusive aspect. Setting up an automated phone survey like Cleveland is effective in gathering meaningful results quickly and efficiently, but if this method is used, we suggest supplementing it with another form that allows citizens to say more. A supplement could be in the form of mail-in responses where citizens that participate in the phone survey are mailed a response form to answer more questions where they can fully respond. This can be done through live mail or through electronic mail. Another possible method is to solely use one of the mail options. The electronic form may be a more efficient and cleaner means to complete a survey, but it would be a moot point if no one has the proper contact information for the citizens. Lastly, as discussed later in this section, should Pittsburgh decide to survey Neighborhood Civic Associations as their initial base study, it would be effective to manually distribute surveys during meetings with return envelopes. Additionally, any way to personally deliver surveys at community gatherings or meetings of some sort would be the most certain way. To conclude the distribution section, a phone survey is effective, but should be supplemented if chosen. Our suggestion is to distribute surveys via mail routes if it is not possible to hand deliver surveys at community gatherings to ensure their receipt.

First and foremost with a survey, there must be clarity in questions. Terms such as "satisfaction," "privacy," "surveillance," "surveillance cameras, "acceptable," and "adequate" need to be clearly defined, otherwise the results will be ambiguous and leave more questions unanswered. This initial survey should be used to determine what the current satisfaction is with Pittsburgh Police Department and set that as a baseline for moving forward. In order to determine satisfaction, questions should probe citizens on what they value from a police department, what their chief concerns are, how well the police department is handling those, and what improvements can be made. From there, the survey should ask citizens what they view as an acceptable level satisfaction and compare that to the baseline of where satisfaction currently is. Lastly with regards to these types of questions, there should be a series of questions directly asking about the trust citizens have in their police and the visibility of their police. These types of questions give valuable insight as to where the community stands in their relationship with the police department and will help to gauge where the relationship can improve moving forward and just how responsive the community is what their police are implementing.

In addition to these very important topics, there needs to be questions surrounding current opinion on surveillance and privacy. Without this knowledge, there is no baseline for the progression of neither domestic surveillance technology nor the conversation with the community. It should be understood what the prevailing opinion is regarding individual privacy and individual rights, even if the opinions overstate their legal or moral boundaries. Citizens need to know their rights are not being ignored, thereby demonstrating that law enforcement understands they have a duty with regards to citizens' privacy rights.

In terms of where this survey should be initially used, we suggest using a broad demographic, whether that is a specific geographic region of Pittsburgh or polling from multiple areas but not everyone from each area. A more effective tactic would be to start in certain areas where public response will be high based on data from participation in elections so a strong baseline can be built. We also suggest utilizing Neighborhood Civic Associations to reach communities. This may be a smaller scale, but it allows for tremendous opportunity to bleed into the community and rally a people to participate and create an open dialogue needed for this issue.

MINNEAPOLIS, MINNESOTA

Description of City

We chose to look at the city of Minneapolis, Minnesota as a comparison city to Pittsburgh. As Midwestern Rust Belt cities situated on important regional rivers, Minneapolis and Pittsburgh share several economic traits. In particular, both cities have a history as regional manufacturing centers, but have in recent years moved towards more service-oriented economies.[91] Minneapolis and Pittsburgh also have similar demographic patterns: as of the 2010 census, the total Minneapolis population was approximately 382,000.[92] Minneapolis' population was 63.8% white, while Pittsburgh's was 66.0% white; Minneapolis was 18.6% black or African American, and Pittsburgh was 26.1%, with the majority of the discrepancy here made up by a

larger Hispanic or Latino population in Minneapolis. The two cities also had a similar poverty rate (22.5%) from 2008 to 2012. The major area of difference is in relative prosperity; in Minneapolis, median household income was approximately $10,000 more than Pittsburgh's, although per capita income was only around $4,000 greater in Minneapolis than in Pittsburgh.

Like Pittsburgh, many areas in Minneapolis have experienced the phenomenon sometimes referred to as revitalization or gentrification. In Minneapolis, the Uptown area, previously a center of art and visual culture has shifted to one more focused on mainstream consumerism and expressions of wealth.[93] In a web article, Minnesota Public Radio (MPR) describes a similar process in Northeast Minneapolis, historically a low-income and racially diverse area.[94] To combat the process of gentrification, the city of Minneapolis has implemented the Northeast Minneapolis Arts Action Plan, a long-range 15-year proposal to help keep artists in the neighborhood. However, MPR points out that this does not address the racial aspects of gentrification, and is pessimistic about the prevention of gentrification through only focusing on the arts community. In a Macalester College study, researchers found that these efforts have somewhat prevented the rapid gentrification of Northeast Minneapolis, but there has been an increase in home value (potentially pricing out the arts community) and mortgage applications filed by whites in the area.[95] While there is little data available on any impact surveillance may have on gentrification or vice versa, the similar processes of gentrification in both Minneapolis and Pittsburgh make Minneapolis an excellent comparison to use in formulating policies for Pittsburgh.

Ecosystem of Surveillance

The Minneapolis Police Department (MPD) employs various surveillance technologies. These technologies include WiFi-enabled CCTV cameras,[96] license plate readers,[97] squad car cameras, Taser cameras,[98] ShotSpotter,[99] and mobile (trailer-mounted) cameras.[100] The City of Minneapolis directly owns 250 cameras, which are typically placed in commercial areas and on high-traffic streets, and in addition to these directly owned cameras, any camera that has an IP address and is connected to the Internet can be used to mine data. This is in juxtaposition with Pittsburgh's current policy where cameras we know of are hardwired through and accessible through CCTV. According to Deputy Police Chief Rob Allen, the Minneapolis Police Department (MPD) "can access right now… an infinite number of cameras."

The MPD is working on a number of ways to expand their video capability: they use portable police cameras, which can be up and running in under an hour, in addition to regular fixed cameras, and are currently working to pair ShotSpotter technology with automated cameras, so that the cameras will turn in the direction the ShotSpotter audio technology triangulates the origin of the gunshot. Starting in 2011, the MPD began an initiative to implement mobile cameras, mounted on 30-ft poles, each rising from an approximately 4x3x3 generator in a wheeled trailer; some have lights to illuminate the parks/streets on which they are placed. These mobile cameras, which the MPD owned 7 of in 2011, cost $29,000 apiece and can be deployed in less than an hour. They are able to connect to WiFi and are meant to augment rather than replace the stationary camera system in the city. Footage from the cameras is

monitored in the MPD's Strategic Information Center, which keeps and observes all of the city's surveillance data.[101] This is in contrast to the City of Pittsburgh's surveillance data, which is kept and observed by the Pittsburgh INP Department.[102]

In addition, the city is currently in the process of approving a pilot program to evaluate the use of police body-worn cameras.[103] Before the body-worn camera pilot program can be implemented, the MPD is required to complete a draft of Standard Operating Procedures for the pilot, and will publish this draft to the public prior to the implementation of the pilot. At the end of the pilot, there will be a full review before city-wide implementation. This review is meant to evaluate whether the body-worn cameras have a significant worthwhile impact on the MPD's effectiveness. [104]

Code of Ordinances and Governance

According to a Minneapolis *Star Tribune* article, there are restrictions on camera placement: the police do ask if neighborhoods want cameras before installing them, but the article does not clarify the process used to gauge community acceptance/interest.[105] Mobile cameras are placed according to crime trends, and the police believe they are a more effective crime deterrent than traditional fixed cameras, with criminals reacting as if there were a police officer on the corner.[106] Neither state nor city law requires the police to notify the public that they are being captured on video when mobile cameras are placed on city streets and in public spaces, and suspicious behavior caught on camera can be used as probable cause for a search.[107]

The Minnesota Data Practices Act requires all public government information, any information that is not classified, an infringement on privacy, or necessary for an active legal case, to be made available to the public. In accordance with this act, the MPD allows certain types of data to be requested, including surveillance footage.[108] Among the types of data that can be requested are squad camera video, street camera video, and Taser camera video. Anyone with knowledge of a specific incident can request information (in fact, it is unclear whether there even needs to have been an incident to receive information – the incident information requested appears to be intended for footage identification purposes). Requests are subject to a flat fee at the time of submittal, varying based on what type of data/footage is requested. There are technological limits on how long data can be stored, and thus on how long data is available for request: 90 days for squad camera video, as these records are not stored for longer periods (there is no information provided on how long Taser video is stored).[109] The MPD explicitly cannot require the requestor to identify themselves or even to provide a reason for the request;[110] any information provided is intended to aid in identifying the correct footage and allow for communication on the status of the request. While this allows for some transparency in the police's surveillance, there may be issues in terms of the availability of access to the general public - in specific cases (albeit unlikely), it may be possible for abuse of access. As illustrated below, a case like this occurred in 2012, when license plate tracking information was still classified as public information.

Community Response

In 2012, Minneapolis's largest newspaper, the *Star Tribune*, reported on the MPD and other city police agencies' use of license plate readers. The reporter was able to access data on his own license plate and found that his license plate had been captured seven times over the course of a year. So long as the license plate is known, anyone can request data on that license plate (note that this no longer appears to be the case, as license plate records do not appear on the Data Request Form).[111] A week later, the reporter tested this out by requesting data on the Minneapolis Mayor's license plate, and found that the mayor's license had been captured over 40 times.[112] After the story broke, the mayor called for, and received, reclassification of license plate data as private rather than public, so that only the subject can request the data.

Analysis

As demonstrated with the license plate tracking situation from 2012, if surveillance data is too readily available then citizens may experience an acute loss of control over their private lives. Regardless how strongly an individual feels about the government collecting their personal information through surveillance, it is likely that they would prefer to keep at least some of this information hidden from the general public. However, if anyone is allowed uninhibited access to surveillance data, any personal information the government has collected – even information the individual may prefer to keep private – will be available to the public. This is a general concern in cases of indiscriminate surveillance footage analysis, and is an especial concern in cases of targeted search – for example, a targeted search could be used by an employer to collect data on employees' religious beliefs, or could be used by a domestic abuser attempting to locate their victim. Although this may not be possible given the current technologies employed in Minneapolis (as shown in the Data Request Form, the requestor must already be aware of an incident in order to request footage, unlike the ability to request all data on a specific license plate), the development of commercially available facial-recognition technologies could give rise to a similar situation. While transparency in terms of use and policy may be desired, it is important to ensure that this transparency does not go too far in making information on specific persons broadly available to the public.

We therefore recommend that all publicly accessible information be thoroughly screened and personal identifiers eliminated from the data prior to distribution. We further recommend that Pittsburgh City Council take into consideration the creation of a separate subsection of the Department of Innovation and Performance (INP) responsible for this that is specifically trained to not abuse access to such personally identifiable data. The Public Safety Camera Review Committee would be most apt to serve as an oversight for this branch of INP and surveillance collection policies.

In addition, as mentioned above it is currently unknown what impact surveillance may have on gentrification or vice versa. For example, surveillance footage being used for probable cause may be able to be used to exclude certain 'undesirable' persons from gentrifying communities by identifying their very presence as suspicious; for this reason, gentrifying communities may either demand more surveillance in order to identify suspicious individuals, or

may use already in place surveillance systems to exclude particular individuals. More research, and perhaps cautious policy measures, may be needed to identify the impact this may have on communities and minimize any impact it may already have. We recommend the City of Pittsburgh partner with local universities to continue to research the impact surveillance systems have had on community cohesion before developing and instating any community-specific surveillance systems plans. We also recommend engaging the public in a public forum prior to any instatement of surveillance, which would impact the citizenry through surveying their everyday activities, and then incorporating the voiced concerns of the citizens into a surveillance action plan.

OAKLAND

Description of City

According to the U.S. Census, Oakland's has a population of 406,000 people, as of 2013. This means that the 55.79 square miles of Oakland have only about 100,000 more inhabitants than the 55.37 square miles of Pittsburgh, which makes it a decent comparison for two cities of almost exactly the same size. Demographically, Oakland is slightly more diverse than Pittsburgh, as 34.5% of the population is white, compared to Pittsburgh's 66%. In Oakland, the following two most populous demographics are African Americans, making up 28% of the population, and Hispanics, making up 25.4% of the population. In Pittsburgh, the second most populous ethnicity is also African American with 26.1%, followed by Asians, making up 4.4% of the population. The poverty level in both cities is very similar, with 20.3% of the population living below the poverty line in Oakland, and 22.5% in Pittsburgh.

Ecosystem of Surveillance

The use surveillance equipment in the city of Oakland did not become particularly salient to members of the community till the Department of Homeland security gave federal grant money to develop the Domain Awareness Center for the city. Originally, the purpose of the Domain Awareness Center was to monitor the Port of Oakland because it was designated a potential terrorist target by the federal government. But, on July 30th, 2013, the City Council of Oakland decided to include the entire city of Oakland within the DAC's jurisdiction. The expansion of DAC would have utilized CCTV cameras, license plate readers, shot spotter, live traffic cameras on the freeway and street, and red light cameras. All of these technologies would have been available for the DAC, which in essence would be one central surveillance hub for the entire city of Oakland. The City of Oakland felt the DAC was a necessary upgrade to their emergency operations center (EOC), which officials claimed was outdated and obsolete. A major function of the DAC according to the City Council was to aid the coordination and response time for emergency services (Oakland PD, Oakland Fire Department, etc.). In addition, DAC could be used for a potential crime prevention tool by law enforcement because the DAC's ability to monitor particular groups or people as they amassed or moved throughout the city.

The Oakland City Council approved the expansion of the DAC without a data retention policy and a privacy code in place to protect the citizens. The lack of privacy laws and provisions to prevent against the unwarranted and unlawful surveillance of citizens generated a great deal of public outcry against the DAC.[113] The Oakland City Council voted down the expansion in early 2014, limiting the DAC to monitor only the Port of Oakland. Surveillance equipment now in use by the DAC for the Port of Oakland includes integrated CCTV system, a spatial mapping system, and truck management system. A citizen's commission has been created since the City Council vote to be put in charge of drafting a surveillance technology and community safety ordinance for the City of Oakland.

Code of Ordinances and Governance

A citizen's commission created a draft for an Oakland surveillance ordinance by modeling it after Seattle's surveillance equipment ordinance, which covers all types of surveillance equipment, and not one specific piece of equipment. Seattle's ordinance lays out data management protocols, and operation and acquisition protocols. The data management protocols require departments to adopt written protocols to address data retention, storage, and access of any data obtained by the use or surveillance equipment. Operation and acquisition protocols require city departments to obtain Council approval for the proper deployment, acquirement, and use of surveillance equipment. There were no enforcement protocols written into the Seattle Surveillance Code discussing the potential repercussions for violations of the provisions laid out.

The major addition to the Oakland code of Ordinances compared to the Seattle code is the addition of enforcement protocols. Additionally, several aspects of Oakland's code promote democratic oversight of government surveillance. These policies could be helpful in ensuring that privacy rights are being respected, and reassuring the public that surveillance is both limited and justified, if adopted by Pittsburgh. Most notably, the Oakland code mandates a public comment period prior to the acquisition of surveillance equipment. This provision allows the public to be informed about plans for surveillance equipment to be used in their respective communities. In addition, it allows the public to formally respond to such plans for the use of surveillance equipment and voice their concerns. The second mechanism that assures democratic oversight of government surveillance is that City Council Approval must approve the acquisition and operation of surveillance equipment. Much like getting a warrant, a city department must obtain approval from the Oakland City Council by demonstrating the purpose and use for the proposed surveillance equipment. If approval is granted, then the city department must adhere to the operational protocols contained in this code of ordinances. The third mechanism of democratic oversight is the requirement of transparency reports with provisions laid out to clarify the use of the surveillance equipment and the parameters involving the management and retention of collected data. Independent audits are laid out to help carry out and enforce the use transparency reports. Lastly, enforcement provisions are laid out stating what happens if any person found to be in violation of any section or provision in the ordinance.

Unfortunately, we were not able to perform extensive research into the city of Seattle and the developments of the surveillance code because we discovered the salience of Seattle too late. However, Seattle should be a city of interest to Pittsburgh because the Seattle Surveillance Code of Ordinances was used as a template for Oakland's code of ordinances. As a result, most of the provisions and language laid out in the Oakland Surveillance Code of Ordinances is identical or at least very similar to Seattle's Surveillance Code of Ordinances. The draft of the Oakland Code of Ordinances lays out the data, operational, approval and enforcement protocols. Purpose specification seems to be of the utmost importance regarding how, when, where, and why the surveillance equipment will be used and preventing the unlawful use and retention of collected data. Also of note is that this code of ordinances covers all types surveillance equipment, and not one particular device.

Community Response

As the public became more aware of the expansion of the Domain Awareness Center's purview to the entire city of Oakland, concern and outrage emerge among both Oakland residents and civil libertarians across the nation. Newspapers and Internet sites published numerous op-eds and related news stories chronicling the public's outcry against the DAC. On December 18, 2013, Ali Winston and Darwin Bond-Graham published an article in East Bay Express entitled "The Real Purpose of Oakland's Surveillance Center" in which they argued, following the views of the ACLU of Northern California, that the DAC was set up to control political protests, rather than violent crime as purported by DAC supporters.[114] City officials countered this argument, claiming the DAC was absolutely vital to the city's crime prevention strategy and that civil libertarians were misrepresenting the intentions in order to scare city residents into opposing coordinated surveillance. Despite the strident opposition to the DAC presence being prevalent throughout the entire city, Oakland Mayor Jean Quan fully intends on bringing back the technologies in order to decrease crime in Oakland. In a recent article, she was quoted as saying "We'll bring them back one at a time. This is obviously an issue that is splitting the country. Unfortunately, the poor little video system gets to be the target."[115]

Analysis

After reviewing the research and documents collected about the Oakland DAC, the policies developed in the Seattle Surveillance Code and the Oakland Surveillance Code can be useful for improving Pittsburgh's surveillance and privacy policies. The data, operational, approval, and enforcement protocols laid out in both codes establish a clear process for what can and cannot be done as with the use of surveillance equipment and the data collected. The use of the data and surveillance equipment must be approved by the City Council and have a specified purpose. These protocols are in place to police against the unlawful invasion of privacy with the use of drones or any surveillance technology and make that sure ethical and compliance policies about the use of drones or any surveillance technology are upheld within the local government. Above all else, the both codes establish a transparent process to properly inform the public and others in the local government (Mayor, City Council, City Administrator, etc.) of almost everything that goes on with surveillance technology. Knowing who is going use or who

accessed the surveillance technology, why it is being used, and what the collected information is being used for is all very important for the proper regulation and enforcement of a surveillance policy.

With the rapid advancement in technology, local governments around the United States are incorporating newer surveillance technology into their enforcement bureaus. The City of Oakland is one example where the necessary safeguards were not in place to police the use surveillance technology, leading to a tremendous public outcry that forced the city to scale back its plans. Before Pittsburgh moves forward with surveillance technology, it is important for the city to have policies in place to protect the people from unlawful invasions of privacy and ensure that surveillance equipment and the data collected is properly handled and used. Hence, the Oakland Surveillance Code and the Seattle Surveillance Code can serve as template, in terms of the types of safeguards and provisions that need to be in place for surveillance policy in Pittsburgh.

OTHER INSTRUCTIVE CASES

In this section, we provide an overview of further surveillance technology, focusing on two of the largest and most populous cities in the country: New York City and Chicago. Although these cities are much larger and more diverse than Pittsburgh, it is important to understand how they implemented surveillance measures and how the public reacted to them. Specifically, we look at the use of red light cameras in New York and Chicago, body-worn Cameras in New York and Chicago, SkyWatch in New York, and Operation Virtual Shield in Chicago. The surveillance technologies implemented in New York City and Chicago serve as benchmarks for the rest of the country.

RED LIGHT CAMERAS

As noted previously in this report, automated red light cameras reinforce traffic laws, specifically, they take photos of vehicles that enter or pass an intersection after the traffic signal turns red. After a photo is taken, law enforcement officials review the images taken by the cameras to determine if a violation occurred. Since manufacturers promote these cameras throughout cities and cities that implement them to be helpful in preventing accidents and reducing traffic violations, many citizens automatically assume that these cameras are effective for these purposes. However, there is a lack of data provided by institutions that are not associated with city government to prove a causal relationship between red light cameras and reduced accidents. Pittsburgh has only used red light cameras for about one year. By looking at states, Chicago and New York, that have used red light cameras for longer periods of time, Pittsburgh can learn how to improve and shape their implementation of red light cameras.

The Chicago Department of Transportation (CDOT) handles the installation and maintenance of red light cameras. The CDOT chooses the locations of their red light cameras based on crash data accumulated over a minimum of two years prior to installation. The CDOT also analyzes crash and violation data for a minimum of two years after installation to determine if the cameras need to be relocated. According to the City of Chicago website, right angle (T-bone) crashes have decreased by 47% between 2005 and 2012[116] due to the implementation of red light cameras. The City of Chicago website also provides an interactive map of current red light camera intersection locations[117] as well as video recordings of personal red light violations.

New York's state laws allow for red light cameras at 150 intersections around the city.[118] Besides red light cameras, the city has also installed "dummy cameras" as well as speed cameras. If a driver is captured violating the law by a red light or a speed camera, the driver will be fined $50. New York City does not directly provide a map online that shows the placement of speed and red light cameras, but their citizens have compiled their personal data to create maps of camera locations.[119] As a result, gadgets like GPS systems and automakers like General Motors and Mazda have provided ways to alert drivers of the camera locations after receiving location data from the Internet. Data location can be requested if a driver submits a form to the

Department of Transportation. New York citizens are also allowed to request the installation or removal of a red light camera, or make a complaint about the placement of a red light camera.

Analysis

The installation of red light cameras has proven to be profitable in every city it is adopted. There is little to no independent, scientifically rigorous data available that illustrates red light cameras are successful at improving traffic safety. In fact, there is research that argues that red light cameras might actually increase the amount of accidents taking place at busy intersections. An independent news website called The Expired Meter requested information about a study that the Chicago Department of Transportation conducted on the effectiveness of Chicago's red light camera program. It found that within the two years of installing the cameras the total number of crashes was virtually unchanged and showed that it decreased by about a fraction of one percent: before the installation, there were about 2,072 crashes and after the cameras were installed there were about 2,066 crashes.[120] Also, the study showed that the number of rear end crashes increased from 485 to 697, which is nearly a 44% increase.[121] The red light camera system automatically mails a ticket to the owner of the vehicle, regardless of who operated the vehicle at the time of the traffic violation. The current methods of red light cameras do not always hold the responsible individuals accountable, which can be attributed to the lack of transparency within the system.

Even though Chicago's methods do not show efficacy, it might be beneficial for Pittsburgh to survey areas before, during, and after red light camera implementation to make sure the technologies work well. Chicago's Department of Transportation's transparency in discussing red light cameras has ultimately shown that its methods are somewhat effective since the amount of accidents have decreased slightly. However, in New York there is limited research on the effects of their red light cameras or unintended consequences. The employment of red light cameras is highly lucrative to the local governments that decide to implement them. As a result, citizens and civil liberties advocates should be extra vigilant about ensuring that this technology is benefiting drivers and pedestrians and that strong privacy and data retention policies are in place.

BODY-WORN CAMERAS

Technology has become increasingly crucial to the daily function of law enforcement agencies. More recently, police agencies have undergone scrutiny and public outcry surrounding the fatal shootings of Michael Brown and Trayvon Martin by police officers. Citizens around the country are demanding more transparency and accountability surrounding the interactions of police officers and the public. Police departments are also seeking ways to protect themselves from accusations that they are abusing their power or behaving inappropriately. Body-worn cameras are currently being debated worldwide and across various media platforms. The implementation of body-worn cameras is quickly gaining support around the country and is seen by many as a remedy to policing.

Currently about 4,000 police agencies worldwide are testing or using body-worn cameras.[122] The Rialto Police Department in California became the first agency in the United States to test the effects of body-worn cameras. Body-worn police cameras are very small and capable cameras; they can be mounted on an officer's collar, glasses, tie, or worn as an earpiece. At the end of an officer's shift, the collected audio and video data is downloaded into a remote server and stored to prevent tampering of the records. The implementation of body-worn cameras is an expensive task, departments have to purchase the actual camera and spend millions of dollars for storage costs (depending on the size of the police force). The popularity of body-worn is rapidly growing however. The logistics behind this technology varies by city and is in flux. When do officers hit "record?" When do officers hit "stop?" How long will video be stored for? What privacy issues are involved?[123] These central questions regarding the functionality of body-worn cameras have been only vaguely discussed in the several news articles and research studies recently published.

The Rialto Police is a mid-sized police department that serves a population of about one hundred thousand residents. The major goal of their study was to reduce the use of police force and to measure how cameras affect individual's behavior. The police department monitored their interactions with citizens, and documented when police used force. In order to measure the effects of body-worn cameras, the Rialto Police conducted a two-group study to analyze the impact of body-worn cameras. "The first group, named Experimental-Shifts, required each officer to wear a high definition Body-worn cameras during their shift. Body-worn cameras record all interaction between officer's and the public. The second group, named Control-Shifts, consisted of officers that were instructed not to use body-worn cameras during their shifts."[124] The shifts were randomly assigned to the officers in order to control and stabilize the conditions of the study. In addition, the Rialto study acknowledged that interactions with minors and sexually based offenses should not be recorded. However, the most striking findings of the Rialto study is that the use of body-worn cameras reduced "use-of-force" incidents by 59% and reduced citizens' complaints by 87.5%[125]. These results demonstrate that body-worn cameras reduce the force that police officers use and they also prevent citizens from making false accusations of police brutality. The results of this study are used by law enforcement agencies around the country to gain legitimize their reasons for implementing body-worn cameras.

In August 2013 Federal Judge Shira Scheindlin ruled that New York Police Department's stop-and-frisk program was unconstitutional because it "targeted minority communities."[126] U.S. Judge Shira Scheindlin ordered the implementation of body-worn cameras pilot program following the stop-and-frisk case. NYPD Commissioner Bill Bratton anticipates that body-worn cameras will be useful during trials and also protect both police officers and citizens. New York Police Department (NYPD) became the largest police force to evaluate body-worn camera technology. NYPD's goal is to reduce violent and fatal interactions between police officers and citizens. The pilot program in New York will utilize two different cameras. The Vievu camera model is the same size of a pager and it can be worn on an officer's shirt. The second model is called the Taser, which is smaller camera that can be mounted on an officer's ear, shoulder,

glasses etc. The pilot program enacted by Mayor Bill de Blasio will have sixty officers begin wearing body-worn camera devices (six different precincts)[127]. The precincts that were selected include the 75th precinct in East New York, Brooklyn; the 40th precinct in Highbridge section in the Bronx; the 23rd precinct in East Harem; the 103rd precinct in Jamaica, Queens; and Police Service Area 2, which includes public housing in Brooklyn. A maximum of ten volunteer officers in each precinct will wear one of the camera models. The precincts involved were selected because they displayed a high number of stops based on 2012 data from stop-and-frisk. NYPD officials are currently working out the logistics, including how long the cameras will be turned on and how long digital files will be stored. A private group purchased the sixty body-worn cameras for sixty thousand dollars[128]. However, if this initiative is expanded across the police force then future costs will reach tens of millions of dollars per year simply for file storage.

The Chicago Police Department is currently contemplating whether it should test body-worn cameras on their officers. Chicago police spokesman Marty Maloney stated that the police department is "looking into a pilot program" but there aren't any plans in place yet.[129] The Chicago Police are open to adapting tools that will allow for more transparency within their department. Unlike New York City that has begun its pilot program, Chicago is still monitoring the effects of body-worn cameras throughout the nation. The increase of police-involved shootings across the nation is often used as incentives to implement body-worn cameras. The Chicago Police Department has decided to set up rules to govern these technologies before they began to implement these devices.

The American Civil Liberties Union (ACLU) released a study on the use of body-worn cameras in October of 2013. The ACLU makes the argument that they do not agree with the increase of camera usage for surveillance. However, the ACLU recognizes that body-worn cameras are an entirely different situation and is considered a best practice among law enforcement.[130] The ACLU agrees that body-worn cameras effectively decrease the use-of-force occurrences by police and it is increasingly helpful as evidence during a court proceeding. The ACLU fears that the use of body-worn cameras may have many unintended consequences, especially in regards to privacy rights. Body-worn cameras have the potential risk to infringe on the rights of the police officers that use them. All of their private and public interactions will be on record therefore they have to be careful of their actions and conversations. In addition, the ACLU is concerned about occasions where harmless behavior is being recorded. For example, when "camera-equipped officers are inside people's homes, whenever police enter — including in instances of consensual entry and such things as domestic violence calls."[131]

The ACLU acknowledges that there are negative and positive features of incorporating body-worn cameras. Organizing a set of policies on the use of body-worn cameras is a crucial component that should be addressed before the technology is adapted. The ACLU is concerned about the police officer's ability to control which encounters they decide to record. If the police officers can control this feature, they are able to regulate the narrative, and the accountability benefits of body-worn cameras would no longer exceed the privacy risks.[132] In many of the cities

that have adopted body-worn cameras there are clear methods of how law enforcement agencies will implement this technology, but many lack strong privacy policies.

Analysis

Law enforcement agencies implement body-worn cameras to decrease the use of force by police officers, and to reduce citizen's complaints.[133] According to the Rialto study body-worn cameras have considerably reduced citizen's complaints against the police and the use of force by police officers. In these respects law enforcement agencies are benefiting from employing body-worn cameras. However, there have been virtually no research studies that investigate the citizen's views of this innovative technology. A majority of the perceived benefits of body-worn cameras are relatively untested or incomplete. The expansion of body-worn cameras throughout American cities is happening a lot faster than the policies that are necessary to govern them correctly. Law enforcement agencies have made numerous claims of benefits, but there is limited evidence available to refute or support their arguments. If body-worn cameras are not regulated properly the technology can infringe on the privacy of both citizens and police officers. In May 2012, the Las Vegas Police Department revealed their pilot testing of body-worn cameras. The Las Vegas Police Protective Association, a police union, threatened to file a suit against the police department because the body-worn cameras demonstrate "a change in working conditions," which should be discussed through the union contract.[134] The NYPD union and other similar groups have made consistent claims that reject the implementation of body-worn cameras.

In addition body-worn cameras have proven to be expensive; especially when you incorporate the price of the device, training of police officers to use the technology, and data storage costs. "In a 2012 Department of Justice (DOJ) comparison of camera systems, the Vievu and Taser Axon, two comparable models, cost approximately $900 to $1,000 per unit, though other options ranged from as low as $119."[135] Taser currently advertises body-worn camera models for law enforcement priced around $299 and $499 per device.[136] Agencies that are interested in adopting body-worn cameras must look at the arguments for and against this technology before implementing. Agencies should also collaborate with researchers to design an experimental study, similar to what took place in Rialto California. Consequentially, their needs to be more independent research conducted on body-worn camera technology because many claims remain untested. New York City's pilot program has potential to be the next mainstream study to test the effects of body-worn cameras on a large scale. The regulations of this study have not yet been disclosed to the public. However, the policies they develop to protect privacy may well dictate how successful their pilot program will be in the future.

SKYWATCH INITIATIVE

The New York Police Department has used observation towers under a program called SkyWatch, since 2012. These towers, manufactured by ICx Technologies, provide the police with a better vantage point of the surrounding areas than they would get from ground-based observation. The tower rises out of a van to about 25 feet high. The SkyWatch that the New York Police department uses is equipped with a spotlight and four cameras (one camera in each direction). According to a recent media report, the placement of SkyWatch towers is determined based on general observations of areas, planned protests, conventions or other gatherings of a large amount of people, and as a direct response to high amounts of crime in a certain area.[137]This is a cause of concern, because it could produce a chilling effect for public democratic participation.

There are several benefits to the use of SkyWatch. One major benefit is cost efficiency. NYPD faces increasing costs as it recruits more police officers and pays current police officers overtime. The SkyWatch towers reduce these personnel costs significantly. First and foremost, only one person operates the towers, so fewer police officers are needed to patrol the area where SkyWatch is being implemented. Additionally, the cameras can all Pan, tilt, and zoom so that one police officer can patrol a large amount of area from the tower. In 2012, the basic tower cost $72,171.28 and the cameras cost $18,000.[138] While this may seem expensive, the NYPD police salary is approximately $46,000 for one officer with little to no training. It is self-evident that the towers are a more cost efficient method of patrolling the streets.

Beyond, financial efficiency, the tower itself is more efficient than police officers patrolling the streets because it provides a better vantage point than police officers can get on the ground.[139] The implementation of SkyWatch towers correlates with a decrease in police brutality. Additionally Loss Prevention Research Council ran a study that focused on violent crime. Their study found that the SkyWatch is more effective in reducing crime than other methods. The New York Police department claims that the crime rates drop and the community is happy, when the SkyWatch towers are put in place. However, they have yet to provide any statistical, quantitative evidence to show this. [140] Another main benefit of the SkyWatch towers is that it is a mobile unit. Because the towers rise out of a mobile van, they can be put in place anywhere, and then can move to other locations based on where they are needed. This makes the towers much more efficient than stationary cameras.

While there are many benefits to the SkyWatch towers, there are also some serious risks involving their implementation in New York. Of course, the major concern here is the discomfort of citizens, who know they may always be observed. An additional risk is that, because people know that the towers are there, they will simply move to an unwatched area if they want to commit a crime. Another concern would be how police officers could immediately respond to an incident, quickly in order to stop it. The towers may prevent crime, but if an incident happens, there needs to be a plan in place to stop that incident right away, this involves other officers being involved, which may make the towers less cost efficient. Finally, cities must seriously consider the impacts that a technology like SkyWatch will have on the ability of residents to

engage in mass democratic action, as was recently demonstrated by recent demonstrations protesting decisions not to prosecute police officers who have used excessive force against members of their communities. While law enforcement obviously has an obligation to maintain social order, they also have an obligation to safeguard the civil liberties and constitutional rights of the people they are sworn to protect.

OPERATION VIRTUAL SHIELD

Chicago is known as one of the most monitored cities in the world; there are more than 25,000 cameras placed within its city borders[141][142]. Most of these cameras have been implemented as a result of Operation Virtual Shield. Operation Virtual Shield is a joint surveillance effort between the Department of Homeland Security and the Chicago Police Department. The two departments created the Office of Emergency Management & Communications (OEMC) to run this program. This program has networked almost all of its 25,000 cameras to security monitor them in one location, OEMC's 911 center. Operation Virtual Shield combines its cameras with biological, chemical, and radiological sensors to simultaneously provide data to its operations center. The technology OEMC uses to operate Operation Virtual Shield is known as Citywide Video Federation technology. This technology allows homeland security, police, fire, and traffic management incidents to be seamlessly linked together. These cameras are both privately and publically owned, and many differ in function.

About 2,000 of the cameras part of Operation Virtual Shield are known as Police Observation Devices (PODs). PODs are owned by the Chicago Police Department and have the ability to automatically track cars and people by jumping from camera to camera. PODs also have the power to magnify (pan-tilt-zoom "PTZ") and the capability of facial recognition. They are also known to detect gunfire while they happen by using wireless technology.[143] There is no explanation how this is possible, but the Chicago Police Department states it is possible. Older PODs are placed in boxes marked with the Chicago Police Department logo and topped with blue flashing lights, however, newer versions of PODs are more discrete. PODs were originally introduced in 2003 to locations where there were a high number of public violence incidents and narcotics-related incidents.

Besides Operation Virtual Shield, Chicago implements other surveillance methods. Starting from 2011, Chicago was the first U.S. city to allow residents calling 911 to send photos and videos of the incidents from their cell phones to OEMC. This procedure is known as Txt2Tip.[144] The tips the Chicago Police Department receives are anonymous. This technology allows residents to report crimes and provide more information about crimes while protecting their personal identity, which allows them to stray away from danger. Txt2Tip encourages the community to get engaged and directly communicate with the police department. Also, Members of the Chicago Police Department have begun wearing body cameras. Aside from body cameras, the Chicago Police also use their police cars as surveillance tools. There are cameras and voice recording devices present on all sides of the outside and inside of the vehicle.

Even though the City of Chicago owns a majority of these cameras and claims that their operations are in line with the First and Fourth amendments, there are no other explicit laws or regulations available to the public that regulates these methods. After the ACLU of Chicago proposed camera rules in 2011,[145] the Chicago police adopted two of the proposals stated in the rules: officers may not use cameras to monitor areas where no legally protected reasonable expectations of privacy exists, and officers ma not base the use of video enhancement or tracking capabilities on individual characteristics such as race or national origin. Such rules may be useful references for Pittsburgh when it decides to implement more cameras. Despite the adoption of two proposals, the Chicago police department and the Chicago city government have provided little transparency into their surveillance methods. There are no laws or regulations in Chicago that prohibit facial recognition technology, there are no periodic audits that evaluate the effectiveness of cameras reducing crime or achieving legitimate government purposes.

A 2011 study done by the Urban Institute: Justice Policy Center and funded by the U.S. Department of Justice found that Chicago needed to address three needs to properly go about using their extensive surveillance system: inclusion of citizens in the planning stages of camera implementation; the need for more training that can help attorneys use camera footage in court; and, the judicious integration of cameras with other new crime control technologies[146] . To address these needs, the study suggested public hearings, community meetings, and efforts towards transparency. The study overall stated that there was no proof in crime rate decrease after implementation of an extensive surveillance system in Chicago.

Overall, the use of surveillance technology in Chicago does not seem to be as effect, or as protective of individual rights, as it could be. The lack of communication between the government, institutions, and its citizens has forced the implementation of surveillance methods to be unjust and violation of privacy rights to Chicago citizens. The ACLU of Illinois “believes that Chicago does not need a camera on every sidewalk, in every block, in every neighborhood. Rather, our city needs to change course, before we awake to find that we cannot walk into a bookstore or a doctor's office free from the government's watchful eye."[147] In the Chicago Tribune quoted local citizen Lamont Williams, who doesn’t believe crime has declined because of the cameras as saying,, “Maybe they should have invested in more officers.”[148] There are no statistics to prove that Chicago’s surveillance methods have been extremely successful – Chicago has not released any statistics that indicate that crime rates have reduced. Chicago’s methods of implementing red light cameras seem to be the most successful measure taken. The Chicago Department of Transportation aggressively analyzes data before and before and during implementation to make sure that the cameras are used well and to their best ability. The CDOT also provides citizens with footage and information online. To further help its citizens understand the use of red light cameras, the CDOT has provided a ‘misconceptions vs. realities’ chart to elucidate common misconceptions many drivers have a bout red light cameras and accidents caused by right-angle turns. Apart from the CDOT’s methods, the first step towards a better way of using Chicago’s surveillance methods is communication with its citizens.

DRONE TECHNOLOGY AND GOVERNANCE

In this section, we examine drone technology and how it has been used in surveillance by both private and government entities throughout the United States. We chose to focus primarily on Dayton, OH because it is a leader in drone technology and operation, due to the presence of Wright-Patterson Air Force Base within its city limits. We also analyze currently pending legislation in Ohio that focuses on regulating drone use by the police. Outside of Ohio, we briefly explore drone use in St. Louis, MO, another hub of this technology. Although Pittsburgh currently does not use drones or have plans for drones in the very near future, many cities are moving towards this technology for comprehensive surveillance and Pittsburgh might do so in the future.

DAYTON, OHIO

Description of City

Dayton, Ohio has a population of 141,359 with a median age of 33.5. [149] Dayton is 51.7% white and 42.9% Black with an area of 55.65 square miles. Compared to Dayton, Pittsburgh has over twice as many people, a greater population density, slightly more square miles and a different breakdown of the population. This clearly shows that Dayton is not a comparison city based on size or population. However, we focused on Dayton because of the insight it can provide on the use of drone technology and community response to additional technology used for surveillance.

Ecosystem of Drone Surveillance

Because we are focusing on drones when discussing Dayton, Ohio, this section will provide an overview of drone surveillance and technology in Dayton. Sinclair Community College, located in Dayton, is considered a leader in providing technical training in drone operations and developers and have partnered with Ohio State University to create a unique unmanned aerial system degree. With this 2-year degree, students are trained in both creation and flight of drones.[150] Sinclair Community College has received millions of dollars in U.S. government funding for drone training and technology.[151]

In 2014, Dayton hosted a three-day conference (Ohio UAS Conference) on drones in which there were 70 exhibitors from all over the world.[152] One major conclusion that can be drawn from this event is that the commercial market is expanding rapidly. More than 700 people attended the conference, including representatives of companies, law enforcement agencies, and the general public. The conference showcased a wide variety of aerial technologies including quadcopters and blimp drones.[153] This conference allowed law enforcement officials to learn about new technology for potential implementation in the future.

Dayton's most common drone technology, used by both the public and private communities, is the quadcopter. Dayton Law Enforcement has tested a new drone technology that improves upon the quadcopter and allows the operator to find and track a specific target for

a significant amount of hours. The Dayton police department used this technology to watch the crowds at a rally where Senator John McCain spoke while he was running for president in 2008. During demonstrations, rallies, and protests, Dayton law enforcement have looked to use this expansive drone technology. Persistent Surveillance Systems, a security company, which uses this technology and is located in Dayton. Dayton law enforcement has turned to this company to provide the drone technology. However, government officials have pushed back because of the cost of maintaining and using the new drone technologies.[154] Dayton law enforcement has not provided information about the training procedures for drone operators nor collection procedures of the data that is obtained.

City Ordinances and Governance

In researching the regulation of drone technology in Dayton, we looked at the city's Code of Ordinances. The Code of Ordinances does not directly address drones, nor does it contain a privacy policies or regulation of surveillance in general. We attempted to find additional governing documents or policies, however there were none available. The lack of policies and governance concerning use of surveillance in Dayton, is concerning from the perspective of transparency and accountability.

Community Response

In August of 2014, a medical helicopter was taking a patient to the hospital, but was delayed by a private drone hired by a public park to take pictures of the property. The drone operator violated FAA guidelines by accidently preventing the helicopter from getting to the hospital for over nine minutes. The patient was medically stable after the helicopter arrived at the hospital, but with a different injury the wait time could have proved fatal.[155] Earlier in April of 2014, another private drone, hired for governmental reasons, intercepted a medical helicopter. Both these incidents caused community outrage and a call for the FAA to create guidelines as soon as possible. While many times the drone operators are innocent and are just unsure of the airspace, it is still a problem because it can cost lives of patients or can cause further problems.[156]

As a result, Dayton has been the focus of Congressional efforts to push the FAA to integrate drones into city laws and policies. Although the military is currently only testing drones within the confines of the air force base, there is potential for drone use in the city in the future and there is a community push for legislation to ensure if this does happen the citizen rights will be respected. The president of a local pro-drone organization stated use of drones if there is a question as to the legitimacy of that use, "reasonableness and common sense is going to prevail."[157] Although this statement was made in good faith and was made in a effort to support drone use by the Dayton police, no context was provided to back up this claim.

Privacy lawyers in Dayton are outspoken that privacy policies must be in place before drones can be used or there will be significant issues of privacy. Further, civil liberties organizations are pushing for legislation that will limit the use of the drones by police and ensure privacy rights. The ACLU of Ohio has stated that drone use is only acceptable if "their use is limited and won't violate anyone's privacy."[158] Further, civil liberties organizations are

supporting legislation in order to curtail the use of drones without a warrant or in places where people have a legitimate expectation of privacy.[159] With regards to the potential drone use by law enforcement, the National ACLU has focused on individual privacy rights and ensuring that the government does not infringe upon these rights. In the talking points provided by the ACLU to local chapters, they indicate that "Drones should be prohibited from indiscriminate mass surveillance, with their use by police only permitted where there are grounds to believe they will collect evidence relating to a specific instance of criminal wrongdoing, or in emergencies." Further, as with other civil liberties platforms, the National ACLU is concerned about the potential marginalization for traditionally profiled groups.

Analysis

Although Dayton is not a good comparison for Pittsburgh in terms of size or population, Dayton's ongoing debate on the use of drones for increased surveillance can provide a useful framework for how Pittsburgh might deal with increasing technological advances. Because of the increase in law enforcement use of drones as well as community use of drones, community groups have been pushing for increased legislation. For Pittsburgh, it is important to understand that there must be a balance between protecting individual privacy rights and enabling appropriate surveillance. In Dayton, law enforcement officials used drones and additional surveillance technology before policies or legislation were in place. Because of this, there was a significant amount of push back and concerns about privacy rights being violated. Moving forward, if Pittsburgh is going to incorporate and begin to use new surveillance technologies, proper procedures for collection of data as well as when this technology will be used must be in place prior to use. Although Dayton has not had significant problems with the police using the drones for unlawful purposes, without a comprehensive code to govern their use, the police can have free reign without a check to ensure rights are not violated. We suggest that if Pittsburgh attempts to implement drone technology, the public is made aware of the potential. Further the public should be allowed an opportunity to express concerns and suggest how policy should be created.

OHIO STATE LEGISLATION

Analysis of Ohio State Legislation as a Model for Local Adoption in Pittsburgh

Two bills recently submitted to the Ohio State legislature offer provisions for the use of drones. Though written for state government, these bills contain numerous provisions applicable to the structure of local government. In fact, the bills sometimes apply the language of "government subdivisions" to include local law enforcement, analogous to the Pittsburgh DPS.

House Bill No. 207

House Bill No. 207, introduced to the Ohio State Legislature by Representative Rex Damschroder of District 88 and currently pending, provides for the regulation of the law enforcement applications of drones.[160,161] The bill's provisions are dual. The first subsection details the individual immunities of government employees in providing information for use in

criminal cases and the liabilities of the political subdivisions that contain them. This component of the bill confers immunity from civil liability to the prosecuting attorney in a criminal case and all employees of that attorney's office or any law enforcement agency "that might otherwise be incurred as a result of providing information on criminally injurious conduct," with the exception of the section of the same bill dealing with the regulation of drone use by government entities.[162]

The second subsection of the bill is its drone policy, which categorically prohibits the operation of drones by law enforcement agencies or individuals acting on their behalf except in the three cases specifically authorized by the legislation itself. Importantly, authorization of any kind extends only to unarmed drones.[163] The bill also broadly prohibits governmental use, "in any trial, hearing or other proceeding," of information collected through unauthorized drone use.[164]

In connection to its stated exception to blanket civil immunity, the bill establishes appeal mechanisms against abusive or unauthorized drone operation by involving "civil action" against any individual or government agency within state purview. Notably, proceedings and damages claimed thereby are not subject to sovereign immunity, fully involving the state and its political subdivisions in liability for drone use by law enforcement.

One authorized case requires a search warrant and specifies that the use of the drone must be in accordance with that warrant; no interpretation is provided by the bill as to how a drone's capabilities translate into the boundaries of a warrant.

The two other cases[165] derive from emergency circumstances. In the former, the bill requires a determination of the U.S. Secretary of Homeland Security that "credible intelligence indicates … high risk of a terrorist attack."[166] The latter requires "a reasonable suspicion that swift action is needed to prevent imminent harm… or to forestall the imminent escape of a suspect or the destruction of evidence." The criteria for such suspicion are not specified by the code, contrarily to the first case (see footnotes), and no oversight or accountability process is described save for the implicit regulatory effect of civil suits against violators.[167]

The proposed HB 207 legislation extends to all remotely controlled or unmanned aircraft and, though particular to the operation of drones by law enforcement, provides oversight mechanisms, which are in themselves generalized to all government entities.[168] Its terms derive conceptually from the refinement of blanket immunity into specific and exclusively defined areas of civil liability delineated by authorizations of drone use, which are in turn enforced only by the direct implications of selective liability.

Senate Bill No. 189

This bill expands in part upon the same section of the Revised Code as HB 207, authorizing drone use on the same three bases and maintain the absolute prohibition on armed craft. [169] However, SB 189 provides a more extensive oversight structure (albeit not explicitly integrated into any government hierarchy at the municipal or state level) for the determination of authorized use, particularly in emergency cases involving terrorism or other imminent danger to

individuals.[170] More generally, drone operators are required to make annual reports on the use of particular drone units and all related applications for authorization.

The bill also expands on the cases in which information obtained through drone operation may be disclosed for diverse government purposes, in contrast to the wholly negative definition of authorized disclosure provided by HB 207. In service to the criteria for government use of information collected through drone operation, SB 189 identifies parameters of consent, urgency and privacy. Alternately, the bill permits the disclosure of all information collected by a drone not used as evidence in the exercise of any legal authority of the state or a political subdivision nor applied for any intelligence purpose.[171]

The bill provides for individual consent to drone surveillance by permitting the use of information gathered pursuant to "a written statement … giving the employee permission to operate the unmanned aerial vehicle for purposes of acquiring information" provided by the person subject to drone surveillance.[172] In this case, the individual intended to be subject to surveillance must provide the consent. The bill does not specify whether individuals incidentally recorded by such surveillance must also provide their consent for drone operation to be authorized.[173]

The bill balances general provisions for drone use under the auspices of a warrant[174] with emergency situations, "in which there is an immediate threat to the life or safety of a person" and requiring the time-sensitive deployment of drones or disclosure of information gathered thereby.[175] Like HB 207, the bill distinguishes between emergency situations identified by the drone operator, which must be subsequently verified by a supervisor or justified by post-facto documentation.[176] In notable contrast to the language of HB 207, the warrant requirement is expressly extended to cases involving terrorism or organized crime.

SB 189 mandates the confinement of drone use to public areas except where warranted or warrantable, in contrast to HB 207 whose non-warrant based authorizations made no explicit or implicit distinction between public and private spheres.[177] SB 189 also provides criteria for the use of drones within the limits of a warrant and specifies that justification for a warrant is necessary (demonstrated on a post-facto basis) in emergency cases, even if such cases prevent the possibility of securing a warrant in advance of drone use.

SB 189 further specifies cost justification and reporting measures for the use of drones by "any department or agency… or political subdivision" of Ohio.[178] For individual operators and agencies alike, it stipulates an investigative response to alleged violations of the bill's provisions and the determination by the agency or a court of any appropriate disciplinary measures against the operator or agency, albeit within an entirely unspecified latitude.

ANALYTICAL CONCLUSIONS AND RECOMMENDATIONS

This section will provide our recommendation synthesized from our research. We have divided the recommendations into three distinct groups: statutes and policies, law enforcement procedure, and community engagement. After each recommendation, we have provided a short summary of the reasons why the recommendation was selected as well as referrals to the appropriate section of the full report.

STATUTES AND POLICIES

We recommend the following for the Pittsburgh code from Analysis of the Pittsburgh Code of Ordinances:

1. Develop and specify the parameters of "a distinct pattern of crime," either within the Pittsburgh Code or as part of a law enforcement protocol related to the Privacy Code

Currently, the Pittsburgh Code specifies that surveillance systems may only be installed in response to an existing pattern of crime rather than to prevent a predicted wave.[179] However, it does not specify what constitutes a distinct pattern of crime. We recommend the establishment of guidelines for identifying the scale and kind of criminal patterns that justify the installation of a new surveillance system. In connection to our recommendation for a review process of law enforcement procedures relating to surveillance, these guidelines could either be established within the Pittsburgh Code itself or developed by the Department of Public Safety (DPS) and subject to review by the Public Safety Camera Review Committee.

2. Establish a more rigorous procedure for posting notices in areas subject to observation

Though the Pittsburgh Code stipulates that areas under surveillance shall be marked with notices to that effect, our research found no evidence that such notices are in fact being posted. This requirement can be strengthened by verifying the presence of a clear notice as part of existing oversight measures; in the absence of such a notice, the operation of all public security cameras pointed to the given area should be suspended until the issue is corrected. [180]

We recommend the following for Operational protocols and Enforcement Provisions for the Pittsburgh Code:

3. Use the Oakland Code as a template for developing operation, acquisition, and enforcement protocols

We recommend that all Pittsburgh city departments be required to seek approval from the City Council prior to the acquisition and operation of any surveillance equipment, expanding on the current oversight mechanisms for the installation of CCTV systems. In order to receive approval, the applicant department must demonstrate to City Council the purpose and need for the specific equipment. This will prevent a single city department from having limitless power to decide what forms of surveillance it would like to use and to ensure that proper oversight exists before, rather than after, the implementation of new surveillance initiatives. We further recommend that current enforcement provisions within Pittsburgh Code of Ordinances be expanded to specify disciplinary measures in response to particular infractions.[181] Because Oakland's surveillance legislation uses the Seattle code as a model, we suggest more generally that the City of Pittsburgh undertake a formal evaluation of surveillance policies and tactics in Seattle.[182]

We recommend the following for implementation of the Pending Ohio State Legislation into the Pittsburgh Code:

In addition to specific city codes, state surveillance legislation can provide a model for Pittsburgh policy; many of the policy challenges faced by state legislators apply at the local level, and promising solutions developed for state implementation can be adapted to address local needs. Though specific to drones, the language of Ohio House Bill 207 (HB 207) and Senate Bill 189 (SB 189) can be generalized to all forms of surveillance for the purposes of adoption by the City of Pittsburgh. We recommend that any expansion of the Code using the language of either bill explicitly extend the adopted or adapted provisions to all surveillance mechanisms and systems used by the city.

4. Adopt Ohio House Bill 207's language dealing with surveillance in cases of terrorist threat and adapt related provisions from Ohio State Bill 189

The existing Pittsburgh Code makes special allowances for surveillance in cases of terrorism or terrorist threat, but does not provide criteria for classifying a threat as terroristic; we recommend that the Privacy Code incorporate the criterion provided by HB 207, that "the United States secretary of homeland security has determined that credible intelligence indicates that there is a high risk of a terrorist attack."[183] If Pittsburgh adopts this section of HB 207, we further recommend that it include the language of SB 189, requiring all drone operations (for the purposes of the Pittsburgh code, all surveillance operations) to "terminate immediately upon obtaining the information" related to the threat situation.[184]

5. Adopt Ohio State Bill 189's oversight provisions for antiterrorist and other emergency surveillance[185]

We recommend that the current emergency provisions of the Pittsburgh privacy code be expanded to provide special allowances and oversight for law enforcement agents who

determine that there is "an immediate threat to the life or safety of a person" and that surveillance use is necessary to assist that person.[186] In order to conduct surveillance without first securing a warrant, law enforcement agents must first submit "a written request for the use of (surveillance systems)… that documents the factual basis of the emergency."[187] Moreover, an official with "supervisory authority or power over the employee" must submit a sworn statement detailing the grounds for the emergency use "not later than forty-eight hours after the employee begins operation."[188] This statement should be issued to "the court of common pleas that has jurisdiction over the person whose life or safety was threatened." If these provisions are incorporated into the Code, we further advise that they be subject to the surveillance oversight clause of the antiterrorism section of SB 189 which specifies "if an application for a warrant or order… is denied, all information from the (surveillance operation)" conducted on an emergency basis "shall be deemed as having been obtained in violation of (the relevant Pittsburgh Code Section)."[189]

We recommend the following for ensuring Publicly Accessible and Personally Identifiable Information:

6. Publically accessible information must be screened for personal identifiers before being made accessible to the public

We recommend that all information gathered through surveillance be thoroughly screened before any form of public released; all personal identifiers should be eliminated from the data prior to public access.[190] We further recommend that City Council consider creating a separate subsection of INP to conduct this screening whose members are specifically trained to not abuse access to such personally identifiable data. The Public Safety Camera Review Committee would be most appropriate to oversee this branch of INP and to review surveillance aggregation policies. Pittsburgh must ensure that surveillance transparency efforts do not go too far in making information on specific persons broadly available to the public.

LAW ENFORCEMENT PROCEDURE

We recommend the following for implementation into law enforcement procedures:

7. Establish a review process within the Pittsburgh Code of Ordinances for law enforcement procedures relating to surveillance

Currently, the Code's oversight provisions apply both to individual cases of abuse of the city's surveillance cameras and the impact of particular surveillance systems on communities.[191] Because the protocols developed by the Department of Public Safety (DPS) directly determine the operational latitude of Pittsburgh law enforcement, they represent the

most efficient mechanism for preventing cases of abuse.[192] Building on the current oversight structure, the Pittsburgh Code could require a periodic review of the DPS's surveillance procedures, working with the DPS to determine the procedures' efficacy in preventing abuse and revising as necessary on that basis.[193]

8. Current staff fill the roles, as defined in the Oakland Code, of a Compliance Officer and Internal Privacy Officer who are in charge of reviewing compliance, surveillance, and enforcement protocols

The compliance officer is a city auditor responsible for reviewing the quarterly reports prepared by the Internal Privacy Officer and conducts random audits to ensure that surveillance equipment staff is abiding by the policy. In addition, the compliance officer is responsible for providing performance audits and quarterly reports to be given to the Mayor, City Administrator, and City Council at least annually. The internal privacy officer is charged with ensuring that surveillance equipment staff abide by the protocols on a day-to-day basis. The officer checks the logs, file reports, and make immediate decisions in circumstances that do not allow time for further review.

The audits and reports provided by the compliance officer and internal privacy officer should provide a comprehensive analysis of the use surveillance technology. The report should also facilitate transparency by keeping public and, especially, Pittsburgh government officials (Mayor, City Council, City Administrator, etc.) well-informed of the dynamics of surveillance use in the city. Knowledge of who uses surveillance technology, who or what it targets, why it is used, and what the collected information is used for is important to the proper regulation and enforcement of surveillance policies. The jobs of the compliance officer and internal privacy officer help ensure proper compliance and enforcement surveillance technology. We recommend that these duties be assigned to current city staff and auditors.

Refer to the appendix in this section for the provisions regarding performance audits, and quarterly reports which have been modified from the draft Oakland Code of Surveillance to fit Pittsburgh's surveillance purposes.

9. Create guidelines for using body-worn camera technology

We recommend that Pittsburgh's law enforcement community create guidelines for using and evaluating body-worn camera technology. These guidelines might eventually become the standard for all Pittsburgh agencies that use body-worn cameras. A policy framework that contains privacy protections for the general public and police officers must be embedded within these guidelines (e.g., when are cameras are turned off, and where will the data be stored?). To this end, we recommend that law enforcement agencies collaborate with researchers to create a structured study (similar to the Rialto study)[194] to test the technology's effects before using it on a large scale. They must also properly train their officers to ensure

that body-worn cameras are utilized correctly and to promote transparency and safety for all involved parties. In order to test the results of body-worn cameras, agencies should conduct surveys and other measures of citizen perceptions of this technology on dimensions of trust, satisfaction and the preservation of privacy.

10. Formal evaluation before implementation of SkyWatch

If Pittsburgh law enforcement agencies considering implementing SkyWatch, we recommend that they undertake a formal evaluation of the advantages and disadvantages of this technology in the context of cost, security, and privacy. Many of the claims made by promoters of this technology remain untested and unsupported. Pittsburgh law enforcement agencies should take a hard look at New York City's experience with SkyWatch, paying particular attention to the public's perception of this technology, especially those who find themselves subject to SkyWatch-based surveillance.

COMMUNITY ENGAGEMENT

Prior to making recommendations regarding a Community Response Survey for the city of Pittsburgh, we conducted research to determine if any public response was already in existence regarding surveillance. Based on our investigations (which were limited to public source records), red light cameras are the only surveillance technology that Pittsburgh residents have been polled about. According to the Public Policy Polling Survey, Pittsburgh residents believed these cameras were a positive force on their community. Furthermore, citizens stated they would be more satisfied if these cameras were used for capturing crimes like rape or a robbery. This information demonstrates a community that sees the value of increased surveillance. Additionally, it reveals a community that values crime prevention and crime deterrence. If this one survey is any indication, it appears that the community is ready to engage in a broader discussion of surveillance in Pittsburgh.

We make the following recommendations for the development of a community satisfaction survey in Pittsburgh, in order to appraise law enforcement relations with citizens.

11. Recommendations for Pittsburgh Community Response Survey – Potential Issues and Delivery

Our research repeatedly highlighted the importance of open communication between the general population and law enforcement agencies regardless of which city we examined. Without this communication, people assume that their rights (including their right to privacy) are being violated more so than if they are well informed about the activities of law enforcement. However, it can challenging to create an open dialogue between law enforcement agencies and citizens (especially those who have traditionally been marginalized

or who feel that the police are in their communities to harass them rather than protect them). However, we feel it is vital to encourage a broad dialogue on domestic surveillance in order to ensure that city residents know what is happening, and have an opportunity to express their views on the policies and procedures enacted by law enforcement agencies and other city departments.

We recommend that City Council undertake a survey of public opinion about surveillance. Based on our research, we argue that: 1) policies should take into account the needs and desires of citizens as well as the prevention of crime; and 2) community engagement will ultimately make local residents more accepting of surveillance regimes than if they find out about the city's actions through the media or activist organizations. It is crucial that the survey be representative of all of the citizens of Pittsburgh, with special attention paid to traditionally marginalized groups as well as other crucial stakeholders like business owners, neighborhood groups, and civil liberties organizations. The details of how the survey would be carried out should be determined in consultation with survey design specialists in government and local universities or think tanks (e.g., Carnegie Mellon, University of Pittsburgh, or the RAND Corporation) and community/neighborhood advocates. We suggest that a diversity of mechanisms be used to reach all stakeholders, including phone, Internet, mail-in and hand-distributed versions of the survey.

12. Recommendations for Pittsburgh Community Response Survey –Survey Questions and Focus Areas

There must be clarity in the questions asked in the survey. Terms such as "satisfaction," "privacy," "surveillance," "surveillance cameras, "acceptable," and "adequate" need to be clearly defined, otherwise the results will be ambiguous and leave more questions unanswered. In addition to questions about surveillance, the survey should address issues of citizen and stakeholder satisfaction with local law enforcement agencies (including their visibility or lack thereof), what they expect from police, and the extent to which citizens trust, and feel comfortable interacting, with the police. With respect to surveillance, citizens and other stakeholders should be asked about their knowledge of technologies being used or considered, whether they believe that the City is doing enough to safeguard individual privacy and individual rights, and if increased surveillance is changing individual or community behaviors in a way that is detrimental to democratic engagement and expression.

13. Public Opinion Deliberative Forum and Survey for implementation of further technology

Public opinion and concerns must be taken into account as more invasive surveillance technologies are brought online. As this occurs, we recommend that the City carefully consider the impact that surveillance systems may have on community cohesion. This task can be accomplished by holding deliberative forums and other outreach activities (such as a

follow-up survey) to gauge public response and gather community input. With the public involved, Pittsburgh can create a society where surveillance is carried out in a way that more acceptable to city residents and stakeholders.

APPENDIX TO THE RECOMMENDATIONS

The following will provide supplemental information about the operational protocols for surveillance equipment and the contents of the performance audits, and quarterly reports provided by the compliance officer and internal privacy officer. The operational protocols have been taken directly from the Oakland Code, but the language for the quarterly reports and performance audits have been modified

Operational Protocols must include the following for City Council consideration:

1. A clear statement describing the purpose and use of the proposed surveillance equipment and an explanation as to why there are no alternatives to use of the proposed surveillance equipment.
2. The type of surveillance equipment to be acquired and used, including its full capabilities, and number of units to be acquired and used.
3. Where a city department proposes to use the surveillance equipment, such as a structure, person, or vehicle it may be attached to or an area within which it may be deployed.
4. How and when a city department proposes to use the surveillance equipment, such as whether the surveillance equipment will be operated continuously or used only under specific circumstances, and whether the surveillance equipment will be installed permanently or temporarily.
5. A mitigation plan describing how the city department's use of the surveillance equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse. The plan shall describe how the city department will prohibit targeting based upon a person's constitutionally protected status, including but not limited to race, religion, ethnicity, gender, sexual orientation, or any other protected status. The plan shall describe how the city department will ensure that lawful activities are not monitored, such as attending a place of worship or a political rally, absent a strong showing for the need to use the surveillance equipment. The showing necessary to monitor lawful activities shall be described in the plan.
6. A description of how and when data will be collected, used, and retained, and who will have access to any data captured by the surveillance equipment.
7. The extent to which activity will be monitored in real time as data is being captured and the extent to which monitoring or analysis of historically recorded information will occur.
8. A public outreach plan for each community in which the city department intends to use the surveillance equipment that includes opportunity for public meetings, a public comment period of no less than 90 days, and written agency response to these comments. City Council approval shall not occur until after the 90 day public comment period and written agency response period has completed.
9. If more than one city department will have access to the surveillance equipment or the data captured by it, a lead city department shall be identified that is responsible for

maintaining the equipment and ensuring compliance with all related protocols. If the lead city department intends to delegate any related responsibilities to other city departments these responsibilities and associated city departments and personnel shall be clearly identified.

10. Whether a city department intends to share access to the surveillance equipment or the collected data with any other government or private entity. No sharing agreement shall be entered into without prior City Council approval.
11. A description of the training to be provided to operators or users of the surveillance equipment.
12. A description of the intended protocols for independent audit and oversight to ensure protocol compliance.
13. A description of the initial cost of the surveillance equipment, and any other costs, annual or otherwise, including but not limited to maintenance, licensing, staff time, and training, and a detailed explanation of the funding source used to cover any cost.

The Compliance Officer is in charge of providing performance audits and quarterly reports that should answer the following questions and describe any corrective action taken or needed:

1. Purpose Specification: How did use of surveillance equipment and the collected data directly advance the specified purpose of the surveillance? If possible, provide specific examples.
2. Data Minimization: Was surveillance equipment used in a manner that did not directly advance the law enforcement's purpose?

3. Data Retention: Was data retained for a lengthier period of time than allowed by the Pittsburgh Code of Ordinances for law enforcement relating to surveillance? If yes, describe how many times this occurred and the specific justifications for each lengthened retention period.
4. Data Safeguards: Was data improperly accessed or used? If yes, provide specific examples. If so, were affected citizens notified?

5. Data Sharing: Was data produced to any outside entity?

    a. If so, how many times was such data produced?
    b. If so, what was the lawful justification (e.g. subpoena, warrant)?
    c. If so, what type of data was produced?
    d. If so, what obligations were imposed on the recipient of such information?

6. Public Access: Number of public records demands and compliance therewith.

7. Cost Justification:

a. Initial startup costs and ongoing annual costs.
b. Have the costs resulted in increased public safety, law enforcement efficiency, or other favorable justification?

i. Number of times the collected data used to bring criminal charges

ii. Type of charges brought
iii. Result of those charges
iv. Specific equipment used that resulted in charges

v. Comparing crime rates in the location before and after the installation of surveillance equipment

8. Dispute Resolution: Have citizen or whistleblower complaints been filed, and if so, what was the nature of the complaints, and were they resolved?
9. Requests for Change: A summary of all requests made to the City Council for approval of the acquisition of additional equipment, software, data, or personnel services including whether the City approved or rejected the proposal and/or required changes to this privacy policy before approval.

The following provisions from Oakland's Code involve quarterly reports to be provided by the Internal Privacy Officer have been modified to fit Pittsburgh's surveillance purposes.

The audit would include the following:

General statistical breakdown of how the surveillance system was used including:

1. Listing and number of incident records by incident category
2. Average time to close an incident record
3. Number of incidents actionable by surveillance staff vs. number of incidents non-actionable and/or false alarms.

Crime statistics for the incidents where the collected data was used including:

1. The number of times data was archived for potential criminal investigations
2. The number of times data was exported for potential criminal investigations[195]

How many times data was shared with non-City entities (e.g., the federal government) including:

1. The type of data disclosed

2. Justification for disclosure
3. The entity to whom the data was disclosed and who disclosed it
4. Date and time of disclosure.

System Access Rights Audit

1. Verification that individual user-assigned access rights match access rights
    a. Policy for user's designated surveillance staff role.
2. Review of surveillance staff's role access rights policy to judge appropriateness for surveillance staff role duties.

ACKNOWLEDGEMENTS

We would like to thank:

- Dr. Jay Aronson for his guidance and mentorship;
- Dr. Robert Cavalier for his enthusiasm and support of our work;
- Councilman Dan Gilman for his accessibility and support;
- Lt. Larry Scriotto, Officer Guy Johnson, and Dec. Joseph Bernarding, for their invaluable insights;
- Dr. Danielle Wenner, for her guidance and support;
- Brian Hoffer, of the Oakland Privacy Group, for his insight on surveillance in the city of Oakland;
- Lastly, we would like to thank Pittsburgh's City Council for allowing us to present our findings and recommendations.

BIBLIOGRAPHY

Journal Articles

Davidson, Mark. "Gentrification as Global Habitat: A Process of Class Formation or Corporate Creation?" Transactions of the Institute of British Geographers, New Series, Vol. 32, No. 4 (2007): 490-506. JSTOR (http://www.jstor.org/stable/4626267).

Donohue, Laura K. "Anglo-American Privacy and Surveillance." *The Journal of Criminal Law and Criminology*, vol. 96, no. 3 (Spring 2006): 1059-1208. *JSTOR* (http://www.jstor.org/stable/40042805).

Huey, Laura. "False security or greater social inclusion? Exploring perceptions of CCTV use in public and private spaces accessed by the homeless." *The British Journal of Sociology,* vol. 61, issue 1 (2010): 63-82. *JSTOR*. doi: 10.1111/j.1468-4446.2009.01302.x.

Ratcliffe, J. H., Taniguchi, T., & Taylor, R. B. "The crime reduction effects of public CCTV cameras: A multi-method spatial approach." *Justice Quarterly,* no. 26 (2009): 747-770.

Roe, Linda K. and Robert E. Rucker. "Human Ecology and Urban Revitalization: A Case Study of the Minneapolis Warehouse District." Mid-American Review of Sociology, Vol. 15, No. 1 (1991): 1-16. JSTOR (http://www.jstor.org/stable/23252934).

Schwartz, Adam. "Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy." Northwestern Journal of Technology and Intellectual Property 11, no. 2 (2013): 45-60. http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1182&context=njtip.

Walby, Kevin. "How Closed-Circuit Television Surveillance Organizes the Social: An Institutional Ethanography." *The Canadian Journal of Sociology*, vol. 30, no. 2 (Spring 2005): 189-214. *JSTOR* (http://www.jstor.org/stable/4146130).

Welsh, Brandon C. and David P. Farrington. "Effects of Closed-Circuit Television on Crime." *Annals of the American Academy of Political and Social Science*, vol. 587 (May 2003): 110-135. *JSTOR* (http://www.jstor.org/stable/1049950).

Newspaper Articles

"Aerial Searches of Fenced Areas Upheld By Court." *The New York Times*, May 20, 1986. http://www.nytimes.com/1986/05/20/us/aerial-searches-of-fenced-areas-upheld-by-court.html.

Balingit, Moriah. "Some Pittsburgh security cameras are out of service for lack of maintenance." *Pittsburgh Post-Gazette,* March 12, 2014. *ProQuest* (1506595018).

Barber, Barrie, Tiffany Y. Latta, and Andy Sedlak. "Drone disrupts CareFlight landing; experts call for FAA action." Dayton Daily News, August 28, 2014. http://www.daytondailynews.com/news/news/local/drone-disrupts-careflight-landing/ng94n/.

Bauder, Bob. "Pittsburgh City Council OKs payment on surveillance camera bill." *Pittsburgh Tribune*, April 24, 2014. *ProQuest* (1519310719).

Bernstein, David and Noah Isack. “The Truth About Chicago’s Crime Rates.” Chicago Magazine, April 7, 2014. http://www.chicagomag.com/Chicago-Magazine/May-2014/Chicago-crime-rates/.

Byers, Christina. “St. Louis police chief wants drones to monitor city from the sky.” *St. Louis Post-Dispatch,* June 23, 2013. http://www.stltoday.com/news/local/crime-and-courts/st-louis-police-chief-wants-drones-to-monitor-city-from/article_1f0a7488-855d-52cf-9590-03129ce48a06.html.

“Chicago police start using facial-recognition software to arrest suspects.” RT, July 15, 2013. http://rt.com/usa/chicago-police-cctv-surveillance-135/.

“Cops will no longer report to certain crime scenes.” The Huffington Post, February 3, 2013. http://www.huffingtonpost.com/2013/02/03/chicago-911-dispatch-chan_n_2611451.html.

Cullotta, Karen Ann. “Chicago Links Street Cameras to Its 911 Network.” The New York Cites, February 20, 2009. http://www.nytimes.com/2009/02/21/us/21cameras.html?_r=0

"Dayton community college expands drone program." The Columbus Dispatch, August 28, 2014. http://www.dispatch.com/content/stories/local/2014/08/28/dayton-community-college-expands-drone-program.html.

"Drone aircraft use spreads to Northeast Ohio, privacy advocates express concern." cleveland.com, February 12, 2013. http://www.cleveland.com/open/index.ssf/2013/02/drone_aircraft_use_spreads_to.html.

Erbentraut, Joseph. “Chicago’s Controversial New Police Program Prompts Fears of Racial Profiling.” The Huffington Post, February 25, 2014. http://www.huffingtonpost.com/2014/02/25/chicago-police-home-visits_n_4855319.html.

Gorner, Jeremy. "Officers' Body Cameras to Pose Tough Issues for Chicago Police." Chicagotribune.com, September 5, 2014. http://www.chicagotribune.com/news/ct-body-cameras-police-met-20140915-story.html#page=1.

Greenwald, Glenn. “NSA collecting phone records of millions of Verizon customers daily,” The Guardian, June 6, 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Gurman, Sadie. “Keeping An Eye on Crime: Pittsburgh Developing Camera Network to Peer Down on Waterways, Bridges.” *Pittsburgh Post-Gazette*, September 21, 2008. *ProQuest* (390414755).

Harding, Margaret. "Pittsburgh Police Officers Start Wearing Video Cameras." TribLIVE.com, October 20, 2014. http://triblive.com/news/allegheny/6969202-74/cameras-officers-police#axzz3HbW6II5p.

Harding, Margaret. “Pittsburgh’s surveillance camera program slow going.” *Pittsburgh Tribune*, September 11, 2009. *ProQuest* (382306088).

Heinzmann, David. “New sensors will scoop up ‘big data’ on Chicago.” The Chicago Tribune, June 23, 2014. http://www.chicagotribune.com/news/local/breaking/ct-big-data-chicago-20140621-story.html#page=1.

Hodges, Cynthia. “Surveillance cameras, drones, and street lights in Chicago?” Examiner.com, November 6, 2011. http://www.examiner.com/article/surveillance-cameras-drones-and-street lights-chicago.

Horgan, John. "The Drones Come Home." National Geographic Magazine, March 2013. http://ngm.nationalgeographic.com/2013/03/unmanned-flight/horgan-text.

Kershner, Seth. "Why Is U.S. Military Pushing K-12 Students to Build Drones In Dayton?." Occupy.com, June 18, 2014. http://www.occupy.com/article/why-us-military-pushing-k-12-students-build-drones-dayton.

Kidwell, David. “Shorter yellow times are now the ticket.” The Chicago Tribune, October 9, 2014. http://www.chicagotribune.com/news/ct-red-light-camera-yellow-timing-20141009-story.html#page=1.

Kidwell, David. “City's yellow light change caught 77,000 drivers.” The Chicago Tribune, October 10, 2014. http://www.chicagotribune.com/news/chi-yellow-light-standard-change-20141010-story.html.

Main, Frank. “Chicago first city with citizens sending photos, videos to 911.” Chicago Sun Times. http://www.suntimes.com/news/4264350-418/chicago-first-city-with-citizens-sending-photos-videos-to-911.html#.VDPbKStdVwQ.

McKinney, Matt. “New Minneapolis Cameras Make Thugs Go Elsewhere.” StarTribune, September 26, 2011. http://www.startribune.com/local/minneapolis/130541488.html.

Navera, Tristan. "Organizers praise Ohio UAS conference efforts “. Dayton Business Journal, August 29, 2014. http://www.bizjournals.com/dayton/blog/uas-dayton/2014/08/organizers-praise-ohio-uas-conference-efforts.html?page=all.

“NYPD Installs ‘Sky Watch’ in Harlem Neighborhood.” New York 1. November 21, 2006. http://www.ny1.com/content/news/64500/nypd-installs--sky-watch--in-harlem-neighborhood.

"Ohio college becoming leader in drone technology." Army Times, September 5, 2014.http://www.armytimes.com/article/20140905/EDU/309050047/Ohio-college-becoming-leader-drone-technology.

Parascandola, Roccoo. "60 NYPD Cops Set to Begin Wearing Body Cameras in Pilot Program." NY Daily News, September 4, 2014. http://www.nydailynews.com/new-york/50-nypd-cops-set-wearing-body-cameras-pilot-program-article-1.1927876.

Roberts, Chris. “Getting a Handle on Gentrification in Nordeast.” Minnesota Public Radio, December 6, 2002. http://news.minnesota.publicradio.org/features/200212/06_robertsc_artsplan/.

Roper, Eric. “City cameras track anyone, even Minneapolis Mayor Rybak.” Star Tribune. August 17, 2012. http://www.startribune.com/local/minneapolis/166494646.html.

Roper, Eric. “Police cameras quietly capture license plates, request data.” Star Tribune. August 10, 2012. http://www.startribune.com/local/minneapolis/165680946.html.

Shallwani, Pervaiz. "NYPD Unveil Two Cameras for Officers." The Wall Street Journal, September 4, 2014. http://online.wsj.com/articles/some-nypd-officers-will-wear-taser-vievu-body-mounted-cameras-1409860929.

Singleton, Malik. “Brooklyn Bureau: NYPD Towers May Defuse Cop, Community Friction.” Brooklyn Bureau. February 22, 2012. http://bkbureau.org/2012/02/22/brooklyn-bureau-nypd-towers-may-defuse-cop-community-friction/.

“St. Louis Police Looking Into Using Drones.” *St. Louis KMOX CBS Local,* October 14, 2013. http://stlouis.cbslocal.com/2013/10/14/st-louis-police-pushing-for-drone-surveillance-program/.

Stross, Randall. "Wearing a Badge, and a Video Camera." The New York Times, April 6, 2013. http://www.nytimes.com/2013/04/07/business/wearable-video-cameras-for-police-officers.html?_r=2&.

Stroud, Matt. “The minority report: Chicago’s new police computer predicts crimes, but is it racist?” The Verge, February 19, 2014. http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist.

Sturdevant, Andy. “Yes, Uptown suffers from a personality crisis, but it’s also vibrant and undeniably walkable.” MinnPost, January 25, 2012. http://www.minnpost.com/stroll/2012/01/yes-uptown-suffers-personality-crisis-its-also-vibrant-and-undeniably-walkable.

Tarm, Michael. “Illinois Police Recording Law Blocked By Supreme Court.” The Huffington Post, November 26, 2012. http://www.huffingtonpost.com/2012/11/26/illinois-police-recording_n_2191800.html.

Timberg, Craig. "New surveillance technology can track everyone in an area for several hours at a time." Washington Post, February 5, 2014. http://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.

The Washington Times. "Drone delays landing of Ohio hospital chopper." Washington Times, August 28, 2014. http://www.washingtontimes.com/news/2014/aug/28/drone-delays-landing-of-ohio-hospital-chopper/.

“Watchdog.com’s Bureau Chief Says Red Light Cameras Have Downsides.” CBS Pittsburgh, August 6, 2014. http://pittsburgh.cbslocal.com/2014/08/06/watchdog-orgs-bureau-chief-says-red-light-cameras-have-downsides/.

Yellen, Larry. “Judge throws out red light camera tickets.” Fox 32, August 12, 2014. http://www.myfoxchicago.com/story/26260100/judge-throws-out-red-light-camera-tickets.

Government, Corporate, and Institutional Publications

United States Census Bureau. Minneapolis QuickFacts. Accessed September 28, 2014. http://quickfacts.census.gov/qfd/states/27/2743000.html.

United States Census Bureau. Pittsburgh QuickFacts. Accessed September 28, 2014. http://quickfacts.census.gov/qfd/states/42/4261000.html.

United States Bureau of Labor Statistics. Pittsburgh Area Economic Summary. October 31, 2014. Accessed November 18, 2014. http://www.bls.gov/regions/mid-atlantic/summary/blssummary_pittsburgh.pdf.

United States Bureau of Labor Statistics. Minneapolis Area Economic Summary. September 30, 2014. Accessed November 18, 2014. http://www.bls.gov/regions/midwest/summary/blssummary_minneapolis.pdf.

Minneapolis Police Department. *Data Practices Request Form*. http://www.minneapolismn.gov/www/groups/public/@mpd/documents/webcontent/wcms1p-105981.pdf.

City of Minneapolis. "Video/Photographic and Other Information." Minneapolis Police Department. Accessed September 28, 2014. http://www.minneapolismn.gov/police/records/police_records_video-data.

City of Minneapolis. "ShotSpotter success – Minneapolis Police get results with new technology." Communications Department. January 30, 2007. Accessed October 26, 2014. http://www.minneapolismn.gov/newsroom/newsroom_200701_20070130-nr_spotshotter.

City of Minneapolis. "Shots Fired Maps." Minneapolis Police Department. Accessed October 27, 2014. http://www.minneapolismn.gov/police/statistics/crime-statistics_codefor_shotsfired.

Conference Presentations

Clement, Ted, Sophia Giebultowicz, Matthew Wicklund. "Gentrification in North Minneapolis." Presented to the Department of Transportation. http://www.macalester.edu/dotAsset/d44ea141-578d-4479-b46f-c9a7a6acd017.pdf

Dickinson, Timothy. "The Impact of CCTV on Crime: A Review of the Evidence." Paper presented at the Request of Mayor Francis G. Slay and the Public Safety Director Eddie Roth for the City of Saint Louis as part of the Public Safety Partnership, St. Louis, MO, September 2, 2012.

Government Publications

Cameron, A., Kolodinski, E., May, H., & Williams, N. *Measuring the Effects of Video Surveillance on Crime in Los Angeles, CRB-08-007*. Sacramento, CA: California Research Bureau, 2007.

City of Chicago. "Municipal Code of Chicago." http://www.amlegal.com/nxt/gateway.dll/Illinois/chicago_il/municipalcodeofchicago?f=templates$fn=default.htm$3.0$vid=amlegal:chicago_il

City of Minneapolis. "ShotSpotter success – Minneapolis Police get results with new technology." Communications Department. January 30, 2007. http://www.minneapolismn.gov/newsroom/newsroom_200701_20070130-nr_spotshotter.
City of Minneapolis. "Shots Fired Maps." Minneapolis Police Department. http://www.minneapolismn.gov/police/statistics/crime-statistics_codefor_shotsfired.
City of Minneapolis. "Video/Photographic and Other Information." Minneapolis Police Department. http://www.minneapolismn.gov/police/records/police_records_video-data.
City of Pittsburgh, Pennsylvania. Code of Ordinances – Title Six, Article VIII, 2008. Municode, 2014.
City of Pittsburgh, Pennsylvania. Code of Ordinances – Title One, Article III, 2013. Municode, 2014.
City of Seattle. Ordinance 124142. Seattle, WA. 2013.
Jackson, Frank G. The Future of Public Safety. Cleveland, OH: City of Cleveland Public Awareness Offices, 2011.
NSA Surveillance Resolution, Pennsylvania H.R. 456, Session of 2013.
National Security Agency Resolution, Pennsylvania H.R. 567, Session of 2013.
Ohio House of Representatives. HB 207. Columbus, Ohio: 130th 2014. General Assembly of the State of Ohio, 2014.
Ohio House of Representatives. *Representative Rex Damschroder.* 130th General Assembly of the State of Ohio, 2014.
Ohio Senate. SB 189. Columbus, Ohio: 130th General Assembly of the State of Ohio, 2014.
Pittsburgh City Council District 7. *Councilman Patrick Dowd Votes 'No' on No-Bid $1 Million Police Contract.* Pittsburgh, PA: City of Pittsburgh, 2014. http://www.pittsburghpa.gov/rss/print.htm?mode=print&id=2195.
Public Act 098-0569, Illinois General Assembly. http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=098-0569
The Vehicle Code (Title 75): Chapter 31, Session of 2012. http://www.dmv.state.pa.us/pdotforms/vehicle_code/chapter31.pdf
The Vehicle Code (75 PA.C.S), P.L. 735, Session of 2012. http://www.legis.state.pa.us/WU01/LI/LI/U.S./HTM/2012/0/0084..HTM
United States Supreme Court. *Dow Chemical Co. v. United States: 476 U.S. 227.* Washington, D.C.: U.S. Supreme Court, 1986. https://supreme.justia.com/cases/federal/us/476/227/case.html.
United States Supreme Court. *Hester v. United States: 265 U.S. 57*. Washington, D.C.: U.S. Supreme Court, 1924. http://www.law.cornell.edu/supremecourt/text/265/57.
United States Supreme Court. *Katz v. United States: 389 U.S. 347*. Washington, D.C.: U.S. Supreme Court, 1967. http://www.law.cornell.edu/supremecourt/text/389/347.
United States Supreme Court. *Marshall v. Barlow's, Inc.: 436 U.S. 307*. Washington, D.C.: U.S. Supreme Court, 1978. https://supreme.justia.com/cases/federal/us/436/307/.

United States Supreme Court. *Oliver v. United States*: *466 U.S. 170*. Washington, D.C.: U.S. Supreme Court, 1984. http://www.law.cornell.edu/supremecourt/text/466/170.

United States Supreme Court. *Weeks v. United States: 232 U.S. 383*. Washington, D.C.: U.S. Supreme Court, 1914. https://supreme.justia.com/cases/federal/us/232/383/case.html.

Corporate Reports

ACLU. *You Are Being Tracked: How License Plate Readers Are Being Used to Record American's Movements.* Web: ACLU of Pennsylvania, July 16, 2013. https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf

King, J., Mulligan, D. K., & Raphael, S. *CITRIS Report: The San Francisco Community Safety Camera Program.* Berkeley, CA: University of California Center for Information Technology Research in the Interest of Society, 2008.

Oakland Privacy Group. Oakland Surveillance Code of Ordinances. Oakland, CA: 2014.

Dwyer, Allison M., et al, "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention." Washington, D.C.: Urban Institute Justice Policy Center, September 2011. http://www.urban.org/uploadedpdf/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.pdf.

Motorola. *Safety in Sight: Video Surveillance Protects Cleveland*. Cleveland: Motorola. PDF.

Web Pages and Blog Entries

McKinney, Matt. "New Minneapolis Cameras Make Thugs Go Elsewhere." *StarTribune.* September 26,

2011. http://www.startribune.com/local/minneapolis/130541488.html

Roberts, Chris. "Getting a Handle on Gentrification in Nordeast." *Minnesota Public Radio*. December 6,

2002. http://news.minnesota.publicradio.org/features/200212/06_robertsc_artsplan/.

Sturdevant, Andy. "Yes, Uptown suffers from a personality crisis, but it's also vibrant and undeniably walkable." *MinnPost.* January 25, 2012. http://www.minnpost.com/stroll/2012/01/yes-uptown-suffers-personality-crisis-its-also-vibrant-and-undeniably-walkable

Roper, Eric. "Police cameras quietly capture license plates, request data." *Star Tribune*. August 10, 2012. http://www.startribune.com/local/minneapolis/165680946.html.

Roper, Eric. "City cameras track anyone, even Minneapolis Mayor Rybak." *Star Tribune*. August 17, 2012. http://www.startribune.com/local/minneapolis/166494646.html.

ACLU. "Warrantless Aerial Surveillance in Dayton." ACLU of Ohio - Privacy. ACLU of Ohio. Accessed October 5, 2014. http://www.acluohio.org/archives/issue/privacy.

"American Civil Liberties Union of Minnesota." Privacy & Technology. ACLU of Minnesota. Accessed October 6, 2014. http://www.aclu-mn.org/issues/privacytechnology/.

"American Civil Liberties Union of Pennsylvania." Pittsburgh. ACLU of Pennsylvania. Accessed October 6, 2014. http://www.aclupa.org/chapters/greaterpittsburgh/.

"Automatic License Plate Readers: You Are Being Tracked." ACLU of Ohio - Privacy. ACLU of Ohio. Accessed October 5, 2014. http://www.acluohio.org/archives/issue/privacy.

“Chicago Police – Video Surveillance Case Study.” Mountain Secure Systems. Last Modified 2011. http://www.mountainsecuresystems.com/downloads/Case_Study-Chicago_Police_Deptartment.pdf.

“Chicago Red-Light Enforcement Program Intersection Prioritization Steps for Relocations.” City of Chicago. Accessed October 27, 2014. http://www.cityofchicago.org/content/dam/city/depts/cdot/RLC_New_and_Relocation_Prioritization.pdf.

“Chicago Red-Light Camera Enforcement Program: Misconceptions and Realities.” City of Chicago. Accessed October 27, 2014. http://www.cityofchicago.org/content/dam/city/depts/cdot/Misconceptions_vs_realities.pdf.

“Chicago’s Video Surveillance Cameras: A Pervasive and Unregulated threat to Our Privacy.”ACLU of Chicago. February 2011. http://www.aclu-il.org/wp-content/uploads/2012/06/Surveillance-Camera-Report1.pdf

“ClearMap.” Chicago Police Department. http://gis.chicagopolice.org/.

Clement, Ted, Sophia Giebultowicz, Matthew Wicklund. “Gentrification in North Minneapolis.” Presented to the Department of Transportation. http://www.macalester.edu/dotAsset/d44ea141-578d-4479-b46f-c9a7a6acd017.pdf

"Cleveland Code of Ordinances." American Legal Publishing - Online Library. American Legal Publishing Corporation. Last Modified September 22, 2014. http://www.amlegal.com/nxt/gateway.dll/Ohio/cleveland_oh/cityofclevelandohiocodeofordinances?f=templates$fn=default.htm$3.0$vid=amlegal:cleveland_oh.

"Dayton, OH Code of Ordinances." Municode Library. Accessed October 29, 2014. https://www.municode.com/library/oh/dayton/codes/code_of_ordinances?nodeId=COORDAOH01.

"Dayton, Ohio." (OH) profile: population, maps, real estate, averages, homes, statistics, relocation, travel, jobs, hospitals, schools, crime, moving, houses, news, sex offenders. Accessed October 29, 2014. http://www.city-data.com/city/Dayton-Ohio.html#b.

“DCJS Honored for Crime Analysis Center Initiative.” Criminal Justice of New York. Last Accessed May 24, 2010. http://www.criminaljustice.ny.gov/pio/press_releases/2010-5-24_pressrelease.html.

"Domestic Drones." ACLU of Ohio - Privacy. ACLU of Ohio. Accessed October 5, 2014. http://www.acluohio.org/archives/issue/privacy.

Farivar, Cyrus. "Oakland accepts federal funds for controversial, vast surveillance setup." Ars Technica. Last modified July 31, 2013. http://arstechnica.com/tech-policy/2013/07/oakland-accepts-federal-funds-for-controversial-vast-surveillance-setup/

“Freedom of Information Act (FOIA).” City of Chicago. http://www.cityofchicago.org/city/en/progs/foia.html.

Geeting, Jon. "PPP: Majority Support for Red-Light Traffic Cameras in Pittsburgh." Keystone Politics. July 13, 2013. Accessed October 29, 2014. http://keystonepolitics.com/2013/07/ppp-majority-support-for-red-light-cameras-in-pittsburgh/.

“Gun Involved Violence Elimination (GIVE) Initiative. “ Criminal Justice of New York. http://www.criminaljustice.ny.gov/crimnet/ojsa/impact/index.htm.

Ho, Vivian. "San Jose police 1st in Bay Area with drone." Crime Scene. Last modified July 30th, 2014. http://blog.sfgate.com/crime/2014/07/30/san-jose-police-1st-in-bay-area-with-drone/.

“Illinois Recording Law.” Digital Media Law Project. http://www.dmlp.org/legal-guide/illinois-recording-law.

“Intellistreets.” Illuminating Concepts. Last Modified 2014. http://www.illuminatingconcepts.com/intellistreets/.

“Introduction to the Red Squad Collection at Chicago History Museum.” Chicago History Museum. http://chsmedia.org/media/fa/fa/M-C/Introduction.htm.

Knapp, Alex. "ShotSpotter Lets Police Pinpoint Exactly Where A Gun Was Fired." Forbes. Last modified June 28th, 2013. http://www.forbes.com/sites/alexknapp/2013/06/28/shotspotter-lets-police-pinpoint-exactly-where-a-gun-was-fired/.

"Mayor Bloomberg And Transportation Commissioner Sadik-khan Announce Speed Camera Enforcement Will Begin On The First Day Of School, September 9th." Welcome to NYC.gov. August 26, 2013. Accessed October 28, 2014. http://www1.nyc.gov/office-of-the-mayor/news/285-13/mayor-bloomberg-transportation-commissioner-sadik-khan-speed-camera-enforcement-will#/2.

“Minneapolis Passes Open Data Policy.” Open Twin Cities. Open Twin Cities. Accessed October 16, 2014. http://opentwincities.org/2014/07/31/minneapolis-passes-open-data-policy/.

Missouri Department of Transportation. “Video Cameras at Signalized Intersections: Frequently Asked Questions.” MoDot St. Louis District. Accessed September 29, 2014. http://modot.org/stlouis/links/signalcameras/htm.

"Oakland, California- Code of Ordinances." Muni Code. Accessed October 1, 2014. https://library.municode.com/index.aspx?clientId=16308.

Oakland Wiki. "Domain Awareness Center." Last Modified October, 2013. http://oaklandwiki.org/domain_awareness_center.

“Police Observation Device (POD) Program.” Chicago Police Department. February 23, 2012. http://directives.chicagopolice.org/directives/data/a7a57b33-129f0be8-b5912-9f0ec6e29b6b3727a6d2.html?hl=true.

“PennDOT Funding Programs.” Pennsylvania Department of Transportation. Accessed October 28, 2014.

http://www.dot.state.pa.us/Portal%20Information/Traffic%20Signal%20Portal/FUND.html

“Pittsburgh Survey Results.” Public Policy Polling. July 11-14.2013. Accessed October 29, 2014. http://www.publicpolicypolling.com/PittsburghResults.pdf.

"Privacy and Government Surveillance." ACLU of Northern California. ACLU of Northern California. Accessed October 5, 2014. https://www.aclunc.org/issue/privacy-and-government-surveillance.

"Privacy and Government Surveillance." ACLU of Ohio. ACLU of Ohio. Accessed October 5, 2014. http://www.acluohio.org/archives/issue/privacy.

“RadioLINK.” DID Fusion Center. Minneapolis Downtown Improvement District. Accessed October 21, 2014. http://www.minneapolisdid.com/page/show/608067-did-fusion-center.

“Red Light Camera Enforcement.” Chicago Department of Transportation. Accessed October 27, 2014. http://www.cityofchicago.org/city/en/depts/cdot/supp_info/red-light_cameraenforcement.html.

"Red Light Camera Information or Complaint." Welcome to NYC. Accessed October 27, 2014. http://www1.nyc.gov/nyc-resources/service/2324/red-light-camera-information-or-complaint.

"Safe and Free." Our Issues - Safe and Free. ACLU of Tennessee. Accessed October 6, 2014. http://www.aclu-tn.org/safeandfree.htm.

"Shots Fired Maps." - City of Minneapolis. Accessed October 2, 2014. http://www.ci.minneapolis.mn.us/police/statistics/crime-statistics_codefor_shotsfired.

"SST, Inc.'s Wide Area Protection Overview." Gunshot Detection Technology Overview. Accessed October 2, 2014. http://www.shotspotter.com/technology.

Walker, Ben. "Will Police Body Cameras Prevent the Next Ferguson." The Good Fight with Ben Wikler. September 12, 2014. http://www.thegoodfight.fm.

"Warrantless Aerial Surveillance in Dayton." *ACLU of Ohio - Privacy*. ACLU of Ohio. Accessed October 5, 2014. http://www.acluohio.org/archives/issue/privacy.

Winston, Ali. "Oakland City Council Rolls Back the Domain Awareness Center." East Bay Express. Last modified March 5th, 2014. http://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac.

Winston, Ali. "Oakland surveillance center progresses amid debate on privacy, data collection | The Center for Investigative Reporting." The Center for Investigative Reporting. Last modified July 18th, 2013 http://cironline.org/reports/oakland-surveillance-center-progresses-amid-debate-privacy-data-collection-4978.

Forum/Discussion Lists

Smith, Brian (WPA Opinion Research). Safety Satisfaction Survey. Cleveland, OH: WPA Opinion Research, 2011

“Minneapolis Passes Open Data Policy.” *Open Twin Cities.* Open Twin Cities. Accessed October 16, 2014. http://opentwincities.org/2014/07/31/minneapolis-passes-open-data-policy/.

"RadioLINK." *DID Fusion Center.* Minneapolis Downtown Improvement District. Accessed October 21, 2014. http://www.minneapolisdid.com/page/show/608067-did-fusion-center.

Audio/Visual Publications

CBS Minnesota, "City of Eyes: Your Camera May Help Police Fight Crime," CBS New Video, posted by CBS
Minnesota. Accessed October 17, 2014, http://minnesota.cbslocal.com/video/6857226-city-of-eyes-your-camera-may-help-mpls-police-fight-crime/.

Films/Videos

CBS Minnesota, "City of Eyes: Your Camera May Help Police Fight Crime," CBS New Video, posted by CBS Minnesota, Accessed October 17, 2014, http://minnesota.cbslocal.com/video/6857226-city-of-eyes-your-camera-may-help-mpls-police-fight-crime/.

"Oakland vs. Government Surveillance! Defeating the Domain Awareness Center." YouTube. Posted by "ReasonTV," March 14th, 2014. https://www.youtube.com/watch?v=op5i30M3PLw.

"ShotSpotter - Gunshot Detection System." YouTube. Posted by "AOL," September 14th, 2012. https://www.youtube.com/watch?v=DBHsPwb7pmk.

"Shotspotter System Adds Audio Capabilities." YouTube. Posted by "KRON 4,"May 23rd, 2014. https://www.youtube.com/watch?v=t1gxMGcsOGQ.

"Shotspotter. Oakland Police admits it is always on and records conversation." YouTube. Posted by "wakeupoakland," May 23rd, 2014. https://www.youtube.com/watch?v=ZI6Zh_I3NqQ.

APPENDIX

Privacy in the Technology Age

A Community Forum on Surveillance in Pittsburgh

[Month ##, Year]
[Time]
[Location]

Surveillance Technologies Used in Pittsburgh

The Pittsburgh Police Department currently employs certain surveillance technologies in order to enhance the efficiency of policing. These include:

Closed-Circuit Television (CCTV)

The city of Pittsburgh deploys mounted cameras throughout the city. The locations are not published. Some cameras have signs notifying passersby to the entry to a zone covered by video surveillance while others do not. CCTV cameras can be used to aid in response to crime as well as provide tracking services to the police and government.

Body Cameras

Body cameras are small cameras that are placed on police uniforms or gear to provide video documentation of the interactions between police and the public. Pittsburgh is just starting to implement body cameras into police practices. Cities around the country, such as New York City, are starting programs to ensure compliance with laws by both the police and civilians. In places where body cameras have been used, there has been a significant decrease in crime and complaints about police brutality.

ShotSpotter

Pittsburgh recently introduced this technology. ShotSpotter is a technology that can help police and emergency response units find the location of a gunshot. Microphone technology switches on at the sound of a gunshot and through triangulation, is able to alert emergency response to the location of the shooting. ShotSpotter is used throughout the country to assist police in response to violent crime.

Community Block Watch

The South Side and communities in police Zone 3 are implementing block watches that include video surveillance. This is a collaboration between community members and police to ensure the well being of the citizens. Community members voluntarily participate in this program and purchase the cameras on their own.

Red Light Cameras

Cameras are mounted on traffic lights throughout the city at major intersections. Currently, Pittsburgh has approximately 20 cameras in operation. These cameras are used to ticket drivers who run red lights. Tickets are mailed to the driver's home and are appealable.

Technologies Used in Other U.S. Cities

Drones

Police departments around the country are beginning to experiment with using drone (unmanned areal surveillance) technology to aid in law enforcement. There is a wide range of the capabilities of drones including continuous video and picture surveillance. Many communities have been expressing concern about the trade off between privacy and security. Some communities have rejected drone use, while others have supported it.

Virtual Shield

Virtual Shield is a program that is currently used in Chicago, Illinois. This is the most extensive use of surveillance cameras in the United States and links over 3,000 surveillance cameras. The technology has the ability for facial recognition and detecting crime.

Mobile Surveillance Towers

New York City recently implemented SkyWatch, mobile 25-foot surveillance towers mounted on compact trailers. Each tower includes high definition lighting and four high-powered cameras. The operator can direct one of the cameras, while the other three cameras are stationary.

Discussion Questions

- What surveillance information should be available for the government to view?
- What should be the limits of privacy? What areas or activities should be private?
- Should Pittsburgh expand its video surveillance capabilities? If so, should this be through expansion of existing technologies or addition of new technologies?
- Would you support a community block watch in your area?
- Do you believe the locations of surveillance cameras should be published and/or have posted signage indicating the area is under surveillance?

Legal Terms, Precedent, and Rights

Curtilage

The area immediately surrounding a private dwelling, typically enclosed or otherwise indicated as an area used for intimate activities of the home. This area is considered the boundary of the area in which a person has a reasonable expectation of privacy. While legally protected from unreasonable search and seizure, this protection is generally less stringent than that afforded to the dwelling itself.

Open-fields Doctrine

Area around the home & the curtilage where the individual does not have a reasonable expectation of privacy and warrantless searches are allowed. This includes areas of private property that are not typically associated with intimate activities of the individual's private life. Legally, the distinction between curtilage and open fields is not always clear.

Plain View Doctrine

A legal doctrine that allows an officer to seize without a warrant evidence that is in plain view. In order to apply the doctrine, the officer (1) must be lawfully present in the area of public view (i.e. not trespassing), (2) must be able to lawfully access the evidence (i.e. cannot manipulate objects to enable view), and (3) must have probable cause for believing the evidence is incriminating (incrimination must be obvious).

Sunshine Laws

Laws that are intended to increase government transparency. The Pennsylvania Right to Know Act is intended to guarantee citizens access to public records of government bodies. Starting in 2009, the government has to prove that something is not a public record to deny access under this act.

Privacy vs. Security Debate

There are debates on whether there exists a tradeoff between privacy and security. Some believe that some restrictions on expectations of privacy may be necessary to reach a desired level of security, while others believe that the desired level of security can be achieved without sacrificing privacy, and some think that sacrificing some privacy necessarily includes sacrificing some security.

Pittsburgh Privacy Code

The Pittsburgh Code of Ordinances includes guidelines for the use of surveillance technologies in Pittsburgh. The Code's primary emphasis is on deterrence of "terrorist and criminal behavior". The placements of these technologies are intended to be strategically determined in order to meet the stated goal of deterrence. The rationale to use surveillance technologies is to achieve the goal of deterrence in the most efficient means possible. As part of this, the Code specifically mentions "safeguards to reduce the potential for misuse".

APPENDIX 2: LINK TO SEATTLE SURVEILLANCE CODE OF ORDINANCES

A PDF version of this code can be found at:
http://clerk.seattle.gov/~archives/Ordinances/Ord_124142.pdf

CITATIONS

[1] Deborah Stone, "Policy Paradox: The Art of Political Decision Making," p. 133

[2] Deborah Stone, "Policy Paradox: The Art of Political Decision Making," p. 129-131, 139

[3] In security-based arguments for surveillance, this threat usually involves criminal behavior.

[4] Deborah Stone, "Policy Paradox: The Art of Political Decision Making," p. 146

[5] Predictive surveillance in particular might operate on this principle.

[6] Michel Foucault, "Discipline and Punish," p. 171-172, p. 199-200

[7] Deborah Stone, "Policy Paradox: The Art of Political Decision Making" p. 151

[8] If the individual, for whatever reason, has privacy but cannot engage in the valuable activities it enables, the benefit and therefore the value of privacy is limited or negated.

[9] Alternatively, but not necessarily, this may also involve the individual's surrender of control over what personal information is subsequently made accessible to others; that is, the individual might never surrender specific information but nevertheless give up an element of privacy.

[10] This information must be necessary in that no equivalently effective prevention or mitigation effort could occur without it.

[11] Deborah Stone, "Policy Paradox: The Art of Political Decision Making" p. 145

[12] Paradoxically, such confidence would likely require enough information that surveillance could contribute nothing to the security of the individual.

[13] The legal concept of probable cause incorporates similar reasoning.

[14] Deborah Stone, "Policy Paradox: The Art of Political Decision Making" p. 152-3

[15] The insecurity is absolute in that it involves an imminent threat, which, if unaddressed, is *certain* to cause loss to life and limb. It is universal in that all people are threatened.

[16] McCormick's work provides insight into the infiltration processes that preceded and complemented early wire-tapping. Charles H. McCormick, *Seeing Reds: Federal Surveillance of Radicals in the Pittsburgh Mill District, 1917-1921* (University of Pittsburgh Press), 9, 24.

[17] Christian Parenti, *The Soft Cage: Surveillance in America from Slavery to the War on Terror* (Basic Books, 2003), 99-100, 106, 138-140.

[18] Olmstead v. United States (1928) notably demonstrates this phenomenon – the majority determined that telegraph and telephone communications did not enjoy 4th Amendment protection, on the basis that the wires connecting two devices were not the personal property of either party. The court revised this stance to a doctrine of privacy rights based on the *expectation* of privacy, most notably in Katz v. United States (1967) – almost 40 years later.

[19] "Senate History 1964-Present: January 27, 1975: Church Committee Created," *United States Senate,* Accessed November 11, 2014, https://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm.

[20] "Church Committee,"*U.S. Senate Select Committee on Intelligence,* Accessed November 27, 2014, http://www.intelligence.senate.gov/churchcommittee.html.

[21] "Highlights of the USA PATRIOT Act," *United States Department of Justice,* Accessed November 27, 2014 http://www.justice.gov/archive/ll/highlights.htm.

[22] Christian Parenti, *The Soft Cage: Surveillance in America from Slavery to the War on Terror* (Basic Books, 2003), 201.

[23] Beverly Gage, "What an Uncensored Letter to MLK Reveals," New York Times, November

11, 2014, http://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html?_r=0.

[24] Ibid.

[25] Ibid.

[26] McCormick, Charles H. "Taming The Steel City Wobblies, 1917-1918." In *Seeing Reds: Federal Surveillance of Radicals in the Pittsburgh Mill District, 1917-1921*. Pittsburgh, Pa: University of Pittsburgh Press, 1997.

[27] Ibid.

[28] Ibid.

[29] Felix Stadler, "Privacy is not the antidote to surveillance," Surveillance & Society: 2002, http://www.surveillance-and-society.org/articles1/opinion.pdf.

[30] "Boston Marathon Terror Attack Fast Facts," *CNN*, November 1, 2014, http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts/.

[31] Jon Healy, "Surveillance Cameras and the Boston Marathon Bombing," *LA Times*, April 17, 2013, http://articles.latimes.com/2013/apr/17/news/la-ol-boston-bombing-surveillance-suspects-20130417.

[32] United States Supreme Court, *Weeks v. United States: 232 U.S. 383* (Washington, D.C.: U.S. Supreme Court, 1914): https://supreme.justia.com/cases/federal/us/232/383/case.html.

[33] United States Supreme Court, *Marshall v. Barlow's, Inc.: 436 U.S. 307* (Washington, D.C.: U.S. Supreme Court, 1978): https://supreme.justia.com/cases/federal/us/436/307/.

[34] United States Supreme Court, *Dow Chemical Co. v. United States: 476 U.S. 227* (Washington, D.C.: U.S. Supreme Court, 1986): https://supreme.justia.com/cases/federal/us/476/227/case.html.

[35] United States Supreme Court, *Oliver v. United States*: *466 U.S. 170* (Washington, D.C.: U.S. Supreme Court, 1984): http://www.law.cornell.edu/supremecourt/text/466/170.

[36] The case of Dow Chemical v. U.S. refuted the EPA's use of a contractor of take photographs of a rural, highly secure chemical plant with a highly advanced $22,000 camera after being refused a tour of the plant. The EPA used the contractor instead of seeking an administrative search warrant (circumventing due process). The court ruled in favor of the EPA. (Dow Chemical Co. v. United States)

[37] "Aerial Searches of Fenced Areas Upheld By Court," *The New York Times*, May 20, 1986, http://www.nytimes.com/1986/05/20/us/aerial-searches-of-fenced-areas-upheld-by-court.html.

[38] The standards in question are the mandating of a surveillance warranting procedure to protect the individual from abuses of our clause subordinating the privacy interests of threatening individuals to the security interest of those they might harm. That is, because we cannot know with certainty that an individual is a security risk, we must avoid misapplying the primacy of victim security over potential perpetrator privacy.

[39] Instance-based surveillance, such as Shotspotter technology and red light cameras, which are activated after an occurrence, are exempt from this overview.

[40] Though the case of Katz v. U.S. looks to be a case of a private moment within a public sphere where it is justifiable to be subject to surveillance, it was not. There was a reasonable expectation that no one could hear through the phone booth, and phone booths at the time were societally considered socially acceptable places to have private and meaningful conversations with an

expectation of privacy to exactly what was being said. Therefore, the U.S. government acted unjustly and invaded the privacy of the prosecutor (which follows the ruling of the Supreme Court for this case). United States Supreme Court, *Katz v. United States: 389 U.S. 347* (Washington, D.C.: U.S. Supreme Court, 1967): http://www.law.cornell.edu/supremecourt/text/389/347.

[41] Private systems and neighborhood locations are not available to the public at this time. Interview, Pittsburgh INP Department, September 5, 2014, Sadie Gurman, "Keeping An Eye on Crime: Pittsburgh Developing Camera Network to Peer Down on Waterways, Bridges," *Pittsburgh Post-Gazette*, September 21, 2008, *ProQuest* (390414755).

[42] City Privacy Ordinance 2008; Gurman 2008.

[43] Margaret Harding, "Pittsburgh's surveillance camera program slow going," *Pittsburgh Tribune*, September 11, 2009, *ProQuest* (382306088).

[44] Ibid.

[45] Hanson, 2013

[46] For the year of 2013, Aviro continued to do maintenance work without contract or pay from the city on cameras installed; however, in January, the company stopped. Ballingit 2014.

[47] Ibid.

[48] Timothy McNulty, "Council gives green light to cameras at red lights," *Pittsburgh Post-Gazette*, December 10, 2013, http://www.post-gazette.com/local/2013/12/10/Pittsburgh-City-Council-approves-red-light-cameras-for-pilot-program/stories/201312100139

[49] Ibid.

[50] "PennDOT Funding Programs," Pennsylvania Department of Transportation, Accessed October 28, 2014, http://www.dot.state.pa.us/Portal%20Information/Traffic%20Signal%20Portal/FUND.html

[51] The Vehicle Code (Title 75): Chapter 31, Session of 2012, Accessed December 5, 2014, http://www.dmv.state.pa.us/pdotforms/vehicle_code/chapter31.pdf

[52] The Vehicle Code (75 PA.C.S), P.L. 735, Session of 2012, Accessed December 5, 2014, http://www.legis.state.pa.us/WU01/LI/LI/US/HTM/2012/0/0084..HTM

[53] "Pittsburgh Survey Results," Public Policy Polling, July 11-14, 2013, Accessed October 29, 2014, http://www.publicpolicypolling.com/PittsburghResults.pdf

[54] "Watchdog.com's Bureau Chief Says Red Light Cameras Have Downsides," CBS Pittsburgh, August 6, 2014, http://pittsburgh.cbslocal.com/2014/08/06/watchdog-orgs-bureau-chief-says-red-light-cameras-have-downsides/.

[55] "Red Light Cameras," National Motorists Association, Accessed December 5, 2014, http://www.motorists.org/red-light-cameras/studies.

[56] Title Six, Article VIII, Chapter 680 – General Provisions https://library.muniPittsburgh Code of Ordinances.com/HTML/13525/level4/HORUCHPIPE_TITSIXCO_ARTVIIIPRPOPUSECASY_CH680GEPR.html#HORUCHPIPE_TITSIXCO_ARTVIIIPRPOPUSECASY_CH680GEPR_S680.01PUOBPR.

[57] Chapter 680.01 – Purpose Objectives and Principles.

[58] A note on format: italicized parentheticals are clarifying additions to the original quote.

[59] Chapter 680.1 – Definitions specifies misuse as the operation of a public security camera system in contravention to Chapter 683 – Access to and Use of Recorded Footage.

[60] Title Six, Article VIII, Chapter 683 – Access to and Use of City Recorded Footage.

[61] The Department of Public Safety is given closer treatment in Title One, Article III, Chapter 116 (Article III – Organization more broadly addresses the structure of governance in Pittsburgh).

[62] Title Six, Article VIII, Chapter 681 – Permitted Use of and Limitations on Use of Public Security Cameras

https://www.muniPittsburgh Code of Ordinances.com/library/pa/pittsburgh/Pittsburgh Code of Ordinancess/Pittsburgh Code of Ordinances_of_ordinances?nodeId=HORUCHPIPE_TITSIXCO_ARTVIIIPRPOPUSECASY_CH681PEUSLIUSPUSECA.

[63] Also referred to as the Public Security Camera Review Committee in other sections of Article VIII

[64] Title Six, Article VIII, Chapter 680.2– Definitions

[65] This report's recommendation section deals with the possibility of strengthening the efficacy of the board in order to properly achieve its intended oversight function.

[66] Title Six, Article VIII, Chapter 686 – Notification https://www.muniPittsburgh Code of Ordinances.com/library/pa/pittsburgh/Pittsburgh Code of Ordinancess/Pittsburgh Code of Ordinances_of_ordinances?nodeId=HORUCHPIPE_TITSIXCO_ARTVIIIPRPOPUSECASY_CH686NO.

[67] Chapter 680 – General Provisions

[68] Chapter 681.01 – Permitted Use

[69] The "Principles" subsection of Chapter 680.1 nominally requires a "written request only as set forth herein" but provides for circumvention by "regulations and procedures promulgated by the Director of the Department of Public Safety and the Chief of Police"

[70] Chapter 680.2 differentiates neighborhood public security cameras from "city" public security cameras (also referred to as public security cameras) as "owned by a neighborhood or community group" and identifies the sections of Article VIII to which they are "specifically subject." Notably, neighborhood public security cameras are still "paid in whole or in part with government monies," preserving Article VIII's stated non-applicability to private cameras and systems.

[71] Though access to such footage is specially restricted or deferred to other regulations, Chapter 686 stipulates that the City's use of "footage of public places from private cameras or from public security cameras owned by community groups *(neighborhood public security cameras)*… shall be subject to all the requirements of this article."

[72] Title Six, Article VIII, Chapter 683 – Access to and Use of Recorded Footage

[73] Title Six, Article VIII, Chapter 687 – Public Comment invites written comment on "a particular City installation or the City public camera systems in general." These are to be considered jointly by the Public Security Camera Review Committee and the Chief of Police.

[74] Title Six, Article VIII, Chapter 689 – Sanctions, Enforcements and Remedies

https://www.municode.com/library/pa/pittsburgh/codes/code_of_ordinances?nodeId=HORUCHPIPE_TITSIXCO_ARTVIIIPRPOPUSECASY_CH689SAENRE.

[75] Title Six, Article VIII, Chapter 688 – Existing Systems – Periodic Reviews Required, Review in Case of Misuse or Harm, Alterations or Change in Purpose.

https://www.municode.com/library/pa/pittsburgh/codes/code_of_ordinances?nodeId=HORUCHPIPE_TITSIXCO_ARTVIIIPRPOPUSECASY_CH688EXSYERREREERECAMIHAALCHPU.

[76] This process is separate from review considerations in response to public comment.

[77] Title Six, Article VIII, 681.01 – Permitted Use.

[78] Balingit, Moriah, "Some Pittsburgh security cameras are out of service for lack of maintenance," *Pittsburgh Post-Gazette,* March 12, 2014, *ProQuest* (1506595018).

[79] Ibid.

[80] Motorola. *Safety in Sight: Video Surveillance Protects Cleveland*. Cleveland: Motorola. PDF.

[81] "Cleveland Code of Ordinances," American Legal Publishing - Online Library, American Legal Publishing Corporation, Last Modified September 22, 2014, http://www.amlegal.com/nxt/gateway.dll/Ohio/cleveland_oh/cityofclevelandohiocodeofordinances?f=templates$fn=default.htm$3.0$vid=amlegal:cleveland_oh.

[82] Ibid.

[83] Ibid.

[84] Ibid.

[85] Frank G. Jackson, *The Future of Public Safety*, Cleveland, OH: City of Cleveland Public Awareness

Offices, 2011, 24.

[86] Brian Smith (WPA Opinion Research), *Safety Satisfaction Survey*,Cleveland, OH: WPA Opinion

Research, 2011.

[87] Smith, *Safety Satisfaction Survey*

[88] 2014 Department of Justice investigation report on police brutality in Cleveland

[89] Urban Institute Justice Policy Center Report, 23

[90] Oakland City Council Report, 14

[91] See Tables 1 & 2

[92] United States Census Bureau, Minneapolis QuickFacts, Accessed September 28, 2014, http://quickfacts.census.gov/qfd/states/27/2743000.html.

[93] Andy Sturdevant, "Yes, Uptown suffers from a personality crisis, but it's also vibrant and undeniably

walkable," *MinnPost,* January 25, 2012, http://www.minnpost.com/stroll/2012/01/yes-uptown-suffers-personality-crisis-its-also-vibrant-and-undeniably-walkable

[94] Chris Roberts, "Getting a Handle on Gentrification in Nordeast," *Minnesota Public Radio*, December 6,

2002, http://news.minnesota.publicradio.org/features/200212/06_robertsc_artsplan/.

[95] Ted Clement, Sophia Giebultowicz, Matthew Wicklund, "Gentrification in North Minneapolis,"

Presented to the Department of Transportation, http://www.macalester.edu/dotAsset/d44ea141-578d-4479-b46f-c9a7a6acd017.pdf

[96] Matt McKinney, "New Minneapolis Cameras Make Thugs Go Elsewhere," *StarTribune,* September 26,

2011, http://www.startribune.com/local/minneapolis/130541488.html.

[97] Eric Roper, "Police cameras quietly capture license plates, request data," *Star Tribune*, August 10, 2012, http://www.startribune.com/local/minneapolis/165680946.html.

[98] Minneapolis Police Department, *Data Practices Request Form*, Accessed November 3, 2014, http://www.minneapolismn.gov/www/groups/public/@mpd/documents/webcontent/wcms1p-105981.pdf.

[99] City of Minneapolis, "ShotSpotter success – Minneapolis Police get results with new technology," Communications Department, January 30, 2007, Accessed October 22, 2014, http://www.minneapolismn.gov/newsroom/newsroom_200701_20070130-nr_spotshotter.

[100] Matt McKinney, "New Minneapolis Cameras Make Thugs Go Elsewhere," *StarTribune,* September 26,

2011, http://www.startribune.com/local/minneapolis/130541488.html.

[101] Ibid.

[102] Interview, Councilman Dan Gilman, November 4, 2014.

[103] City of Minneapolis, "Mayor Hodges, Chief Harteau Detail Timeline, Next Steps for Body Camera Pilot Program," Communications Department, September 17, 2014, Accessed October 22, 2014, http://www.minneapolismn.gov/mayor/news/WCMS1P-131162.

[104] City of Minneapolis, "Mayor Hodges, Chief Harteau Detail Timeline, Next Steps for Body Camera Pilot Program," Communications Department, September 17, 2014, Accessed October 22, 2014, http://www.minneapolismn.gov/newsroom/newsroom_200701_20070130-nr_spotshotter.

[105] Matt McKinney, "New Minneapolis Cameras Make Thugs Go Elsewhere," *StarTribune,* September 26,

2011, http://www.startribune.com/local/minneapolis/130541488.html.

[106] Ibid.

[107] Ibid.

[108] Minneapolis Police Department, *Data Practices Request Form*, Accessed December 5, 2014, http://www.minneapolismn.gov/www/groups/public/@mpd/documents/webcontent/wcms1p-105981.pdf.

[109] City of Minneapolis, "Video/Photographic and Other Information," Minneapolis Police Department, Accessed September 28, 2014, http://www.minneapolismn.gov/police/records/police_records_video-data.

[110] Minneapolis Police Department, *Data Practices Request Form*, Accessed December 5, 2014, http://www.minneapolismn.gov/www/groups/public/@mpd/documents/webcontent/wcms1p-105981.pdf.

[111] Eric Roper, "Police cameras quietly capture license plates, request data," *Star Tribune*, August 10, 2012, http://www.startribune.com/local/minneapolis/165680946.html.

[112] Eric Roper, "City cameras track anyone, even Minneapolis Mayor Rybak," *Star Tribune*, August 17, 2012, http://www.startribune.com/local/minneapolis/166494646.html.

[113] "Domain Awareness Center," Oakland Wiki, last modified November 14, 2014, https://oaklandwiki.org/domain_awareness_center#Timeline

[114] Darwin Bond-Graham and Ali Winston, "The Real Purpose of Oakland's Surveillance Center," *East Bay Express*, December 18, 2013, http://www.eastbayexpress.com/oakland/the-real-purpose-of-oaklands-surveillance-center/Content?oid=3789230

[115] Will Kane, "Oakland to limit surveillance center to port, airport," *The SF Gate*, March 6, 2014, http://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php

[116] "Red Light Camera Enforcement," Chicago Department of Transportation. Accessed October 27, 2014, http://www.cityofchicago.org/city/en/depts/cdot/supp_info/red-light_cameraenforcement.html

[117] "Chicago Traffic Tracker," City of Chicago, Accessed September 28, 2014, http://www.chicagotraffictracker.com.

[118] "Legislation: City Control of Street Safety." NYC. Accessed September 26, 2014, http://www.nyc.gov/html/visionzero/pages/legislation/legislation.html

[119] "New York City Photo Enforced Cameras Map," Photoenforced, Accessed October 12, 2014, http://www.photoenforced.com/ny.html#.VH9iDaTF8mU

[120] "Chicago Red Light Camera Study Shows Mixed Reviews," *The Expired Meter*, March 13, 2012, http://theexpiredmeter.com/2012/03/chicago-red-light-camera-study-shows-mixed-results/

[121] Ibid.

[122] Rocco Parascandola,"60 NYPD Cops Set to Begin Wearing Body Cameras in Pilot Program." *NY Daily News*, Accessed September 5, 2014, http://www.nydailynews.com/new-york/50-nypd-cops-set-wearing-body-cameras-pilot-program-article-1.1927876.

[123] Eugene P. Ramirez, "A Report on Body Worn Cameras," Accessed October 14, 2014, http://www.parsac.org/parsac-www/pdf/Bulletins/14-005_Report_BODY_WORN_CAMERAS.pdf

[124] Ibid.

[125] "Self Awareness To Being Watched and Socially-Desirable Behavior," Rialto Police Department, Accessed September 28, 2014, http://www.policefoundation.org/sites/g/files/g798246/f/201303/The%20Effect%20of%20Body-Worn%20Cameras%20on%20Police%20Use-of-Force.pdf

[126] Rocco Parascandola, "60 NYPD Cops Set to Begin Wearing Body Cameras in Pilot Program," *NY Daily News*, Accessed September 5, 2014, http://www.nydailynews.com/new-york/50-nypd-cops-set-wearing-body-cameras-pilot-program-article-1.1927876

[127] Rocco Parascandola, "60 NYPD Cops Set to Begin Wearing Body Cameras in Pilot Program," *NY Daily News*, Accessed September 5, 2014, http://www.nydailynews.com/new-york/50-nypd-cops-set-wearing-body-cameras-pilot-program-article-1.1927876.

[128] Rocco Parascandola, "60 NYPD Cops Set to Begin Wearing Body Cameras in Pilot Program," *NY Daily News*, Accessed September 5, 2014, http://www.nydailynews.com/new-york/50-nypd-cops-set-wearing-body-cameras-pilot-program-article-1.1927876

[129] Jeremy Gorner, "Chicago Police considering Body Cameras," *Chicago Tribune*, September 3, 2014, http://www.chicagotribune.com/news/local/ct-police-body-cameras-met-0903-20140903-story.html.

[130] "Strengthen CBP with the Use of Body-Worn Cameras." American Civil Liberties Union. Accessed October 10, 2014, https://www.aclu.org/sites/default/files/assets/14_6_27_aclu_handout_re_body-worn_cameras_for_cbp_final.pdf

[131] Eugene P. Ramirez, "A Report on Body Worn Cameras," Accessed October 14, 2014, http://www.parsac.org/parsac-www/pdf/Bulletins/14-005_Report_BODY_WORN_CAMERAS.pdf

[132] Ibid.

[133] Ibid.

[134] "Police Officer Body-Worn Cameras: Assessing The Evidence," Michael D. White, Accessed October 7, 2014, https://ojpdiagnosticcenter.org/sites/default/files/spotlight/download/Police%20Officer%20Body-Worn%20Cameras.pdf

[135] "Strengthen CBP with the Use of Body-Worn Cameras." ACLU, Accessed October 10, 2014, https://www.aclu.org/sites/default/files/assets/14_6_27_aclu_handout_re_body-worn_cameras_for_cbp_final.pdf

[136] Ibid.

[137] Malik Singleton. "Brooklyn Bureau: NYPD Towers May Defuse Cop, Community Friction." Brooklyn Bureau. February 22, 2012, http://bkbureau.org/2012/02/22/brooklyn-bureau-nypd-towers-may-defuse-cop-community-friction/.

[138] Ibid.

[139] "NYPD Installs 'Sky Watch' in Harlem Neighborhood," New York 1. November 21, 2006, http://www.ny1.com/content/news/64500/nypd-installs--sky-watch--in-harlem-neighborhood.

[140] Malik Singleton, "Brooklyn Bureau: NYPD Towers May Defuse Cop, Community Friction," Brooklyn Bureau, February 22, 2012, http://bkbureau.org/2012/02/22/brooklyn-bureau-nypd-towers-may-defuse-cop-community-friction/.

[141] "Welcome to Chicago, Most Surveilled City in the World," *NBC Chicago*, April 6, 2010, http://www.nbcchicago.com/news/local/Welcome-to-Chicago-Most-Surveilled-City-in-the-World-89991502.html

[142] Gaudiosi, John. "'Watch Dogs' turns the cameras on NSA fears." *Fortune*, May 27, 2014, http://fortune.com/tag/operation-virtual-shield/.

[143] "Police Observation Devices (PODs)." Chicago Police Department, Accessed December 05, 2014, https://portal.chicagopolice.org/portal/page/portal/ClearPath/About%20CPD/POD%20Program

[144] "Txt2Tip," Chicago Police Department, Accessed October 16, 2014, https://portal.chicagopolice.org/portal/page/portal/ClearPath/Communities/Crime%20Prevention/TXT2TIP

[145] "Chicago's Video Surveillance Cameras: A Pervasive and Unregulated threat to Our Privacy," ACLU of Chicago, Accessed October 2014,
http://www.aclu-il.org/wp-content/uploads/2012/06/Surveillance-Camera-Report1.pdf

[146] Allison M. Dwyer, Nancy G. La Vigne, Samantha S., Lowry, and Joshua A. Markman, "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," Urban Institute Justice Policy Center. Accessed December 5, 2014,
http://www.urban.org/uploadedpdf/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.pdf

[147] Erin Meyer, "ACLU: Chicagoans among most-watched citizens in U.S," *Chicago Tribune*, February 8, 2011, http://articles.chicagotribune.com/2011-02-08/news/ct-met-aclu-surveillance-cameras-20110208_1_surveillance-cameras-aclu-report-facial-recognition-technology

[148] Ibid.

[149] "Dayton, Ohio," (OH) profile: population, maps, real estate, averages, homes, statistics, relocation, travel, jobs, hospitals, schools, crime, moving, houses, news, sex offenders, Accessed October 29, 2014, http://www.city-data.com/city/Dayton-Ohio.html#b.

[150] "Dayton community college expands drone program." The Columbus Dispatch, August 28, 2014, http://www.dispatch.com/content/stories/local/2014/08/28/dayton-community-college-expands-drone-program.html.

[151] "Ohio college becoming leader in drone technology," Army Times, September 5, 2014, http://www.armytimes.com/article/20140905/EDU/309050047/Ohio-college-becoming-leader-drone-technology.

[152] Ibid.

[153] Tristan Navera, "Organizers praise Ohio UAS conference efforts," Dayton Business Journal, August 29, 2014, http://www.bizjournals.com/dayton/blog/uas-dayton/2014/08/organizers-praise-ohio-uas-conference-efforts.html?page=all.

[154] Craig Timberg, "New surveillance technology can track everyone in an area for several hours at a time," Washington Post, February 5, 2014,
http://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.

[155] The Washington Times, "Drone delays landing of Ohio hospital chopper," Washington Times, August 28, 2014, http://www.washingtontimes.com/news/2014/aug/28/drone-delays-landing-of-ohio-hospital-chopper/.

[156] Barrie Barber, Tiffany Y. Latta, and Andy Sedlak, "Drone disrupts CareFlight landing; experts call for FAA action," Dayton Daily News, Accessed October 29, 2014,
http://www.daytondailynews.com/news/news/local/drone-disrupts-careflight-landing/ng94n/

[157] "Drone aircraft use spreads to Northeast Ohio, privacy advocates express concern," cleveland.com, February 12, 2013,
http://www.cleveland.com/open/index.ssf/2013/02/drone_aircraft_use_spreads_to.html.

[158] Ibid.

[159] ACLU. "Warrantless Aerial Surveillance in Dayton." ACLU of Ohio - Privacy. ACLU of Ohio. Accessed October 5, 2014, http://www.acluohio.org/archives/issue/privacy.

[160] The present language of HB 207 is available online, subject to change until the point of formal enrollment by the Assembly. http://www.legislature.state.oh.us/bills.cfm?ID=130_HB_207

[161] Representative Rex Damschroder is a Republican representative to the Ohio state legislature. http://www.ohiohouse.gov/rex-damschroder

[162] All subsequent discussion of immunity and liability within the first subsection addresses the condition of political subdivisions not specifically related to the use of drones and therefore tangential to this analysis.

[163] HB 207 contains two sections, of which the first contains the bill's novel provisions and the second a notice of repeal for particular elements of the State Code external to the language of the bill itself and related only to the discussion of immunities and liabilities.

[164] In this case, unauthorized use involves any violation of the bill's provisions or use in excess of some more limited authorization it might provide.

[165] These cases appear first and third in the order of the bill, but are conceptually connected.

[166] The identification of a terrorist risk is explicitly and uniquely attributed to the secretary of homeland security, and the criteria for such a determination are therefore only those promulgated by the department through its protocols or, if these are not applicable, the autonomous judgment of the secretary. This specification, however indirect, of the provenance of terrorist risk assessment contrasts notably with the imprecision of similar allowances within the Pittsburgh Code.

[167] Without a stated or cited basis for determining reasonable suspicion in this instance, any basis for a civil claim becomes dependent upon a nebulous interpretation of grievances or adverse effects open to wide discretion.

[168] The terms of the bill also specify the use of "aerodynamic forces to provide vehicle lift," essentially negating its applicability to balloons or other lighter-than-air craft that do not generate aerodynamic lift.

[169] The present language of SB 189 is available online, subject to change until the point of formal enrollment by the Assembly. http://www.legislature.state.oh.us/bills.cfm?ID=130_SB_189

[170] Independently of HB 207, SB 189 mandates the operation of drones in compliance with all regulation of airspace and aircraft; this component of the policy may be in anticipation of FAA regulations for drone use.

[171] S.B. 189 Sec. 4561.54 (A) (6). This provision implicitly establishes the boundary if the bill's prohibition on government use of drones by negatively defining a domain of blanket exemption.

[172] Sec. 4561.54 (A) (1). Notably, this section equates the recipient of the written permission, "employee," with the person, also "employee," conducting the surveillance. The transferability of this expression of consent, whether among employees or different governmental agencies, is not addressed by the bill.

[173] This may be particularly relevant to cases in which the consenter engages in criminal activity with others; whereas law enforcement might otherwise need to use the consenter's account to secure a warrant, it may be possible to engage in the warrantless surveillance of accomplices through the consent of one individual.

[174] The warrant in question follows general procedure for the relevant court of common pleas and does not specify special circumstances for authorized drone use relative to other forms of surveillance or intrusion.
[175] The State of Ohio S.B. 189, Sec. 4561.54 (A) (2)
[176] This documentation must take the form of an application for a warrant, submitted within 48 hours of the drone operation. In the event that the warrant application is refused, all related operation and information thereby obtained is considered a violation of the bill's other provisions.
[177] The bill does not invoke a specific warranting process.
[178] S.B. 189, Sec. 4561.58. (A)
[179] As discussed in our analysis of the Pittsburgh Code, this clause applies to the installation of the cameras and not their operation.
[180] If this is not technically feasible, all data collected from those specific cameras should be considered invalid for any government purpose.
[181] If such specifications already exist within the protocols of the Office of Municipal Investigation, we recommend that they be subject to review by the Public Safety Camera Review Committee, which could then make recommendations for specific punitive
[182] Please see the appendix of this report for selections from the Seattle Code. The time limitations of this project prevented us from conducting an in-depth analysis of the policy to complement our study of the Oakland legislation.
[183] HB 207 Sec. 4561.50. (A) (1)
[184] SB 189 Sec. 4561.54 (A) (3) (b)
[185] SB 189 Sec. 4561.54 (A) (2) (a) and (b), (A) (3) (c)
[186] We interpret assistance as the direct prevention of loss to life and limb but recognize other meanings to the word; as a clarifying measure, we recommend specifying the meaning of assistance in this context.
[187] SB 189 Sec. 4561.54 (A) (2) (a)
[188] SB 189 Sec. 4561.54 (A) (2) (b)
[189] SB 189 Sec. 4561.54 (A) (3) (c)
[190] In order to achieve this recommendation, we also advise that the code include clear criteria for determining what constitutes personally identifiable information.
[191]See the "Community Engagement" section for recommendations pertaining to impact evaluation.
[192] See this report's analysis of the Pittsburgh Code of Ordinances for further analysis of the DPS's current role within the privacy policy.
[193] The current Public Safety Camera Review Committee established within the Code of Ordinances could provide an effective forum for implementing this recommendation.
[194] The Rialto study is a recent experimental evaluation of the effect of body-worn video cameras on police practices.
[195] Exported means used elsewhere outside of Pittsburgh