Watching the Watchers: A Crowdsourced Approach to Protecting the Right to Assemble in the Age of Digital Surveillance

BY

Gabriel Brock[1,2]

Professor

James Waldo[1]

December 2023

(Updated January 2024)

[1]Harvard University, School of Engineering and Applied Sciences, Department of Computer Science
[2]Harvard University, Faculty of Arts and Sciences, Department of Government

ABSTRACT

In the face of escalating digital surveillance technologies, the right to assemble freely and peacefully is increasingly under threat. This paper proposes the development of "Watch the Watchers," a crowdsourced platform designed to enhance public awareness of surveillance in major American cities. Inspired by Amnesty International's Decoders model, the platform employs a systematic approach to identify and categorize surveillance cameras, integrating an exposure-based navigation system. The key objectives include accurately tagging cameras, ensuring user privacy by securing internal communication through end-to-end encryption, and optimizing navigation based on surveillance camera exposure. We were inspired by initiatives like Decode Surveillance NYC. Much like the quest to map CCTV cameras in New York City, our method empowers individuals to contribute vital data to a collective effort aimed at preserving civil liberties. We delve into the implications of surveillance on the right to assemble. Our research takes a multidimensional approach, introducing a novel visual model that goes beyond traditional analyses and develops a tool for non-academics to use.

1. INTRODUCTION

> *"The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others."*
>
> Article 21 of the International Covenant on Civil and Political Rights [1]

1.1 Panopticism and Policing

The concept of panopticism, as conceptualized by Michel Foucault, revolves around the idea of a centrally located watchtower from which all individuals within a system can be observed without their knowledge [2]. In the realm of policing, panopticism manifests through the pervasive use of surveillance technologies and practices, enabling law enforcement agencies to monitor individuals in both public and private spaces. Modern policing relies heavily on surveillance mechanisms that parallel the panoptic model. Closed-circuit television (CCTV) cameras, facial recognition technology, and data analytics have become integral components of law enforcement strategies [3] [4]–[8]. The panoptic gaze, facilitated by these technologies, not only monitors individuals but also shapes their behavior through the awareness of potential scrutiny.

Panoptic surveillance reinforces power differentials between law enforcement agencies and the public [9]. The asymmetry of information and control allows the police to dictate and regulate societal norms. Citizens, aware of being under constant surveillance, may modify their behavior to conform to perceived expectations, thus contributing to the self-regulating nature of panopticism [10]. The widespread adoption of panoptic surveillance in policing raises significant concerns regarding privacy and civil liberties. The omnipresence of surveillance technologies challenges the right to privacy, prompting debates about the balance between public safety and individual freedoms. Policymakers and legal scholars grapple with the ethical implications of unchecked surveillance and its potential to infringe upon constitutional rights.

While panopticism enhances the monitoring capabilities of law enforcement, it also demands a corresponding commitment to accountability and transparency. Public oversight, ethical guidelines for technology use, and robust legal frameworks are essential to prevent abuses of power and protect citizens from unwarranted surveillance. Striking a balance between security imperatives and civil liberties is a pressing challenge for contemporary policing. The intersection of panopticism and policing underscores the evolving dynamics of surveillance in modern society. As technology continues to advance, it is imperative to critically assess the ethical and social implications of pervasive surveillance within law enforcement. Achieving a delicate equilibrium between public safety and individual rights requires thoughtful consideration, open discourse, and a commitment to upholding democratic principles in the face of technological progress.

1.2 Chilling Effect of Surveillance on Protesting

The existence of a surveillance-related ‘chilling effect’ is a well-known phenomenon that arises when individuals or groups modify their behavior due to a fear of the consequences that may result if that behavior is observed [11]. Understand the chilling effect of surveillance on protesting, examining how the omnipresence of surveillance technologies, both overt and covert, impacts individuals' willingness to exercise their right to assemble and express dissent. The discussion explores the historical context, the technological landscape, and the implications for civil liberties and democratic societies.

Throughout history, the act of protesting has been a cornerstone of democratic expression, providing citizens with a means to voice dissent, challenge authority, and advocate for social change. However, the history of protest movements is also intertwined with government surveillance, from the monitoring of civil rights activists in the 1960s to contemporary surveillance of various social and political movements. The government has a long history of abusing surveillance tools to intimidate and undermine activists and social movements.

The historical context of government surveillance and its impact on civil liberties is exemplified by the COINTELPRO program initiated by FBI Director J. Edgar Hoover in the 1950s [12]. This program targeted political activists, including civil rights leaders like Martin Luther King, Jr., employing tactics such as wiretapping, disruption, and defamation. The Church hearings in the 1970s exposed COINTELPRO, leading to increased scrutiny and the establishment of the Foreign Intelligence Surveillance Act (FISA) in 1978 to regulate domestic spying. COINTELPRO's legacy underscores the potential of government surveillance to stifle dissent and activism, as seen in its impact on Martin Luther King, Jr. The threat of covert government actions, including wiretapping and smear campaigns, instilled a sense of self-censorship among activists. Fearing potential repercussions, individuals became more cautious about expressing dissenting opinions or engaging in controversial actions, impacting the spontaneity and openness that characterized some protest movements [13][12]. The parallels between historical clashes over surveillance and contemporary challenges, as highlighted by Farai Chideya's exploration of the Bush administration's wiretapping, emphasize ongoing debates on the balance between security measures and protecting individual rights.

In the post-9/11 era, the federal government and local law enforcement engaged in widespread surveillance and infiltration of Muslim American organizations, resulting in unjustified law enforcement investigations and fostering an atmosphere of distrust and fear within the Muslim community. This pattern of surveillance, reminiscent of historical instances such as COINTELPRO, has had lasting implications on the relationship between the government and targeted communities.

The USA Patriot Act, enacted six weeks after the 9/11 attacks, played a pivotal role in expanding the government's surveillance powers and set the stage for a series of measures that significantly enhanced domestic surveillance capabilities [14] [15]. The impacts of these surveillance measures were particularly felt by Muslim Americans [14]. The government, invoking the threat of domestic sleeper cells and extremist activities, deployed undercover agents to monitor mosques, Halal grocery stores, and Muslim student groups. The revelation of these practices, such as the Associated Press uncovering surveillance efforts in 2011, led to lawsuits and court settlements. These legal actions resulted in new rules intended to prevent prolonged intelligence operations on religious and political groups without specific suspicion of criminal activity.

Despite these legal remedies, concerns persist that similar aggressive surveillance techniques are being employed in investigations into movements against police brutality, such as the Black Lives Matter movement [16] [17]. Activists report being interrogated about organizational networks and subjected to inquiries about their activities, mirroring the methods used in the post-9/11 surveillance of Muslim communities. This has led to a sense of déjà vu for those who experienced the earlier wave of surveillance.

The historical context of government surveillance, including the COINTELPRO program targeting civil rights leaders and the post-9/11 surveillance of Muslim Americans, underscores a recurring pattern of overreach and abuse of power. The chilling effect of surveillance on political activism, as seen in both historical and contemporary instances, raises critical questions about the balance between national security imperatives and the protection of civil liberties. By learning from historical responses to government overreach and recognizing the lasting impact on targeted communities, there is an opportunity to shape policies that uphold democratic values while addressing security concerns.

1.2.1 Chilling Effect on Freedom of Assembly

The mere awareness of pervasive surveillance has a chilling effect on individuals' willingness to participate in protests. Fear of reprisals, identification, or stigmatization can deter citizens from engaging in peaceful demonstrations [18]-[20]. This chilling effect undermines the democratic principles that underpin the right to free expression and assembly, impeding the diverse and robust exchange of ideas essential for a thriving democracy.

The use of surveillance technologies in monitoring protests raises legal and ethical questions [21]. Concerns over the potential abuse of power, infringement on the right to privacy, and the disproportionate impact on marginalized communities highlight the need for clear regulations and safeguards. Striking a balance between maintaining public order and protecting fundamental rights remains a complex challenge for policymakers and civil liberties advocates. Surveillance disproportionately affects marginalized communities, exacerbating existing power imbalances [21]. Racial and social profiling, combined with surveillance technologies, can lead to the targeting and intimidation of specific groups, further stifling their ability to exercise their right to protest without fear of retribution [22]–[24].

Preserving the integrity of democratic values, especially the right to assemble, requires addressing the chilling effect of surveillance on protesting. Establishing transparent regulations, fostering public dialogue on the ethical use of surveillance, and advocating for the protection of civil liberties are crucial steps in safeguarding the right to dissent and ensuring a vibrant and resilient democratic society. As surveillance technologies continue to evolve, it is imperative to confront the chilling effect they have on the exercise of fundamental rights. Striking a balance between security concerns and the preservation of democratic values requires a comprehensive approach that prioritizes transparency, accountability, and the protection of civil liberties, fostering an environment where citizens feel empowered to engage in peaceful protest without fear of unwarranted scrutiny or reprisals.

1.3 Surveillance in the 21st Century

In the two decades since 9/11, the American surveillance landscape has undergone a profound transformation, evolving from hypothetical discussions of Orwellian-level "hyper surveillance" to the widespread deployment of advanced technologies [17]:

- **Cameras (Ground and Aerial):** The proliferation of cameras, both on the ground and in the air, has become ubiquitous. Surveillance cameras are now a common feature in public spaces, businesses, and private properties. Additionally, aerial surveillance, often conducted via drones, has expanded, raising concerns about privacy.
- **Closed-Circuit Surveillance Systems:** Closed-circuit television (CCTV) systems have seen widespread adoption, monitoring public areas, transportation hubs, and government facilities. These systems provide continuous surveillance and are often used for crime prevention and investigation.
- **Biometric Surveillance Technology:** The use of biometric data, such as fingerprints, iris scans, and voice recognition, has become integral to surveillance. Biometric technology enables the identification and tracking of individuals, impacting areas from law enforcement to border control.
- Facial Recognition Software and Databases: Facial recognition technology has gained prominence, allowing authorities to match faces captured on camera with existing databases. This technology is controversial due to privacy concerns, potential inaccuracies, and the risk of mass surveillance.
- **Cell Site Simulators:** Commonly known as Stingrays, these devices mimic mobile phone towers to intercept and collect data from mobile phones. Used by law enforcement, they enable location tracking and monitoring of communication activities, sparking debates over privacy and Fourth Amendment rights.
- **Other Technologies:** The surveillance landscape includes a range of other advanced technologies. Predictive policing software uses algorithms to forecast potential criminal activity, while body-worn cameras capture interactions between law enforcement and the public, influencing accountability discussions. These developments underscore the

complex interplay between security, privacy, and the ethical use of technology in modern surveillance.

1.4 Sophisticated Surveillance and Silencing

The American government's historical surveillance tactics have converged with the capabilities of 21st-century surveillance technologies, creating a landscape where advanced tools enable more intrusive monitoring of individuals and groups. The government's history, including post-9/11 surveillance measures, laid the groundwork for an expansion of surveillance practices [15]. In recent years, technologies such as drones, sophisticated cameras, biometric surveillance, and facial recognition have been deployed, allowing for more extensive and targeted data collection. The integration of these technologies into surveillance strategies reflects a convergence with historical practices, where government agencies surveilled and infiltrated various groups. The proliferation of such technologies poses a direct threat to the anonymity and privacy traditionally associated with the right to assemble and protest.

Recent incidents, such as the Phoenix police monitoring protest leaders with drones and surveillance cameras, waiting for them to engage in any conduct that could provide a pretext to arrest them, such as stepping off the sidewalk onto a roadway during a demonstration [25] or New York police using facial recognition software to track a protester to his home, where dozens of officers attempted to forcibly enter without a warrant because he allegedly loudly shouted into a bullhorn at an officer during a demonstration [26] exemplify how 21st-century surveillance technologies amplify historical surveillance tactics and converge with physical policing practices. This convergence raises questions about privacy, civil liberties, and the potential for misuse of surveillance tools. As these technologies become more prevalent, there is a growing need for oversight, accountability, and a reassessment of the balance between national security concerns and individual rights in the digital age.

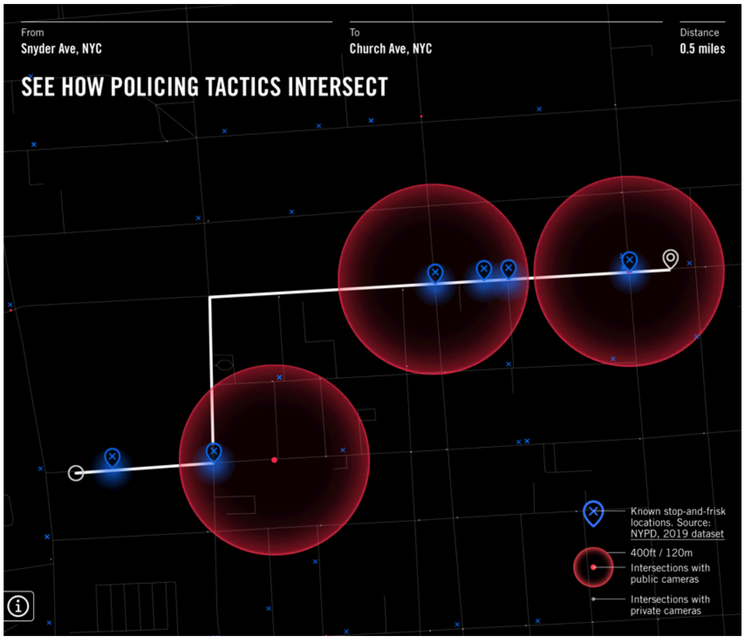

From
Snyder Ave, NYC
To
Church Ave, NYC
Distance
0.5 miles
SEE HOW POLICING TACTICS INTERSECT
Known stop-and-frisk locations. Source: NYPD, 2019 dataset
400ft / 120m
Intersections with public cameras
Intersections with private cameras

Figure 1: Map of NYPD Argus Cameras and Stop-and-Frisk Locations

2. RELATED WORK

Although understanding the effects of surveillance on physical and digital behavior has been a critical topic of research in political science and psychology, few works in the fields of political science and media studies attempt to analyze the impact of modern surveillance on physical protest behavior due to the lack of proper methods and datasets.

While this paper is the first work that develops a tool to allow non-researchers to utilize this analysis in a method that is useful to assembly this is not the first work that quantifies and analyzes the existence of surveillance systems in major metropolitan areas and how this impacts civil expression and assembly to tackle related research questions in political science and tech policy. Extensive research has been conducted on the disparities and biases present in facial recognition technology [21], [24], which has become an increasingly used component of modern policing. The New York Police Department (NYPD) is the most prolific user of camera-based surveillance and facial recognition in policing [27] [28] so it has become a global use case for the effects and proliferation of modern surveillance. The New York Civil Liberties Union has spearheaded the concept of the "camera walk", a survey of cameras within a defined geo-political boundary [29][30], a 1998 study conducted by the NYCLU identified 2,397 video surveillance cameras visible from street level in Manhattan, New York [29]. Another walk conducted five years after 9/11 showed an almost identical number of surveillance cameras was counted in just one area of lower Manhattan that comprises Greenwich Village and SoHo. The 2005 survey identified 4176 public and private cameras below Fourteenth Street, almost six times the 769 cameras counted in that area in 1998 [30]. 292 surveillance cameras were spotted in central Harlem, where there was not a surveilled portion of 125th Street. Similarly, the Surveillance Camera Players published a series of maps of New York City with hand-drawn locations of surveillance cameras throughout the 2000s and 2010s [31]–[33].

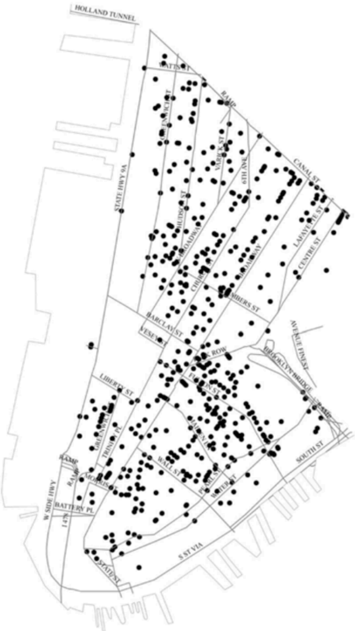


Figure 2: Cameras in the Financial District and Tribeca, NY. This map shows the distribution of video surveillance cameras in the Financial District as of 2005. Each dot represents a camera owned and operated either by the City of New York or by a private entity [30].

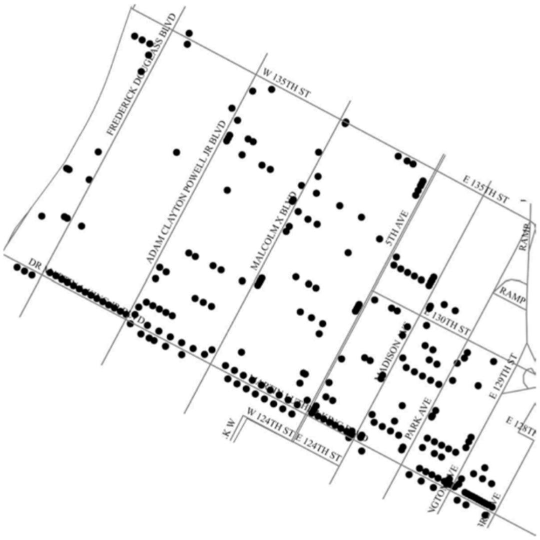


Figure 3: Cameras in Central Harlem, NY. This map shows the distribution of video surveillance cameras in Central Harlem as of 2005. Each dot represents a camera owned and operated either by the City of New York or by a private entity [30].

In the modern era, Amnesty International has developed the digital counterpart of the camera walk. Amnesty International conducted research detailing the New York City surveillance landscape in response to the NYPD's then non-compliance with Freedom of Information

Requests [34] [35]. In 2021, Amnesty International identified 15,280 surveillance cameras at intersections across Manhattan (3,590), Brooklyn (8,220), and the Bronx (3,470). Combined, the three boroughs account for almost half of the intersections (47%) in New York City, constituting a vast surface area of pervasive surveillance [26]. Amnesty International has created a brilliant framework for a tool to empower activists and regular citizens to view how their daily movements are captured.

"A *New York Post* reporter once gathered images from the 200-plus security cameras (both private and government) he passed on a normal Tuesday on the job. At 9:51 a.m. he was caught on film buying coffee at a deli near his Brooklyn apartment. About an hour later, he was captured driving on the Brooklyn Queens Expressway by a Department of Transportation traffic camera. From there he was spotted entering the *Post*'s offices on Sixth Avenue and Forty-eighth Street and riding the elevator to his office. Later that day he was filmed talking to a source while eating lunch in Times Square; taking the subway; having a drink with a friend at a café in Greenwich Village; and renting a DVD on Court Street back in Brooklyn" [36] [30].

Amnesty International developed a digital platform that gave people the opportunity to locate closed-circuit TV (CCTV) cameras across New York City [34]. Volunteers were shown a Google Street View image of a New York City intersection and asked to study the image, tag cameras and classify its type and location.

2.1 Improving the Decode Surveillance NYC Framework

The Amnesty International initial camera walk sprouted several recommendations for improvement to the model. However, we chose to highlight two of their major concerns. Most pressing being the late-stage exclusion of the use of Krippendorff's alpha (α), a method to counteract tagging disagreement. Krippendorff's alpha is a reliability coefficient developed to measure the agreement among observers, coders, judges, raters, annotators, or measuring instruments drawing distinctions among typically unstructured phenomena or assigning computable values to them [37].

Krippendorff's alpha's general form is

$$\alpha = 1 - \frac{D_o}{D_e}$$

where D_o is the observed disagreement among values assigned to units of analysis and D_e is the disagreement one would expect when the coding of units is attributable to chance rather than to the properties of these units. Unlike other specialized coefficients, α is a generalization of several known reliability indices. It enables researchers to judge a variety of data with the same reliability standard. α applies to any number of observers, not just two and any number of categories, scale values, or measures which is why the property is especially useful for quantifying disagreement between taggers, which is a major point of contention for tagging. Amnesty International was unable to utilize Krippendorff's α because of a lack of experience with the model [38]. Implementing the alpha in the analysis model will help to create a more accurate set of data.

Amnesty International also introduced the possibility to use deep learning computer vision to automate the camera using the decoders' answers as training data [39]. Since modeling has already been done, a deep vision model would be able to be reliably tested on the New York data once constructed and once tested generalize to other cities, depending on how similar their cameras and architectures are to NYC's [38]. This will be particularly useful due to the existence of different camera models. Utilization of a deep vision model would help to further improve tagging accuracy but the model itself would have to undergo the same level of training and scrutiny that the human rounds of tagging underwent.

3. PROJECT DESIGN: WATCH THE WATCHERS (WATCH^2)

3.1 Scope of the Platform

To ensure our population bases are large enough to have a sufficient interest in camera tagging, we will only expand preliminary interest to the next four most populous American cities; Los Angeles, Houston, Phoenix, and Chicago, and Boston only including the census-designated cities not their greater metropolitan areas acknowledging that these cities have far different population densities than New York City.

Inspired by Amnesty International, we decided to use Google Street View's API to take the camera survey methodology online – widening access to volunteers and allowing us to cover these cities. Google Street View has the most comprehensive geographic coverage and up-to-date imagery needed for the survey to produce meaningful results [40] [41].

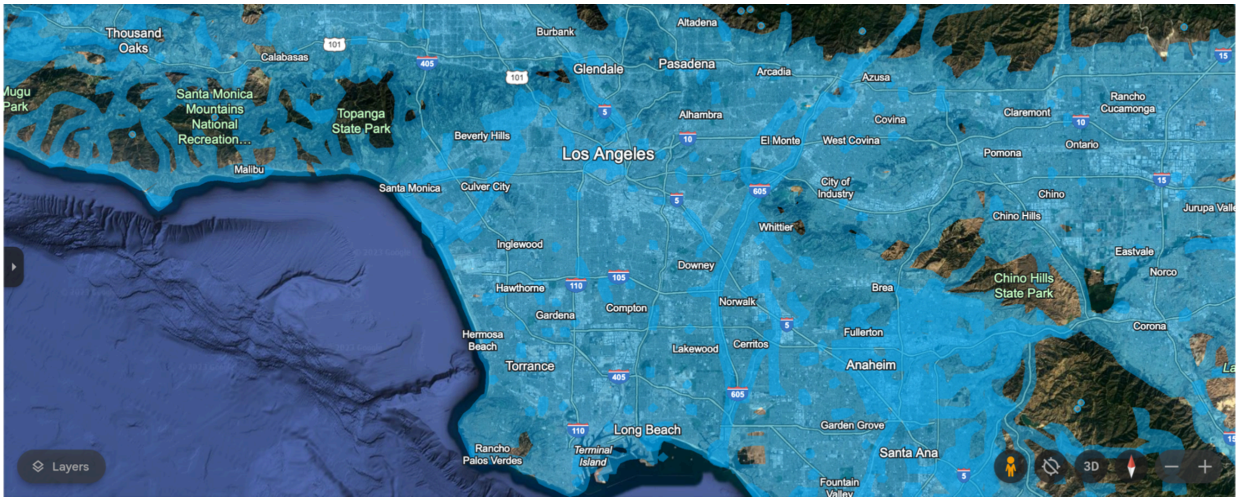


Figure 4: Los Angeles, California. The areas in blue have been imaged by Google Street View © Google Earth

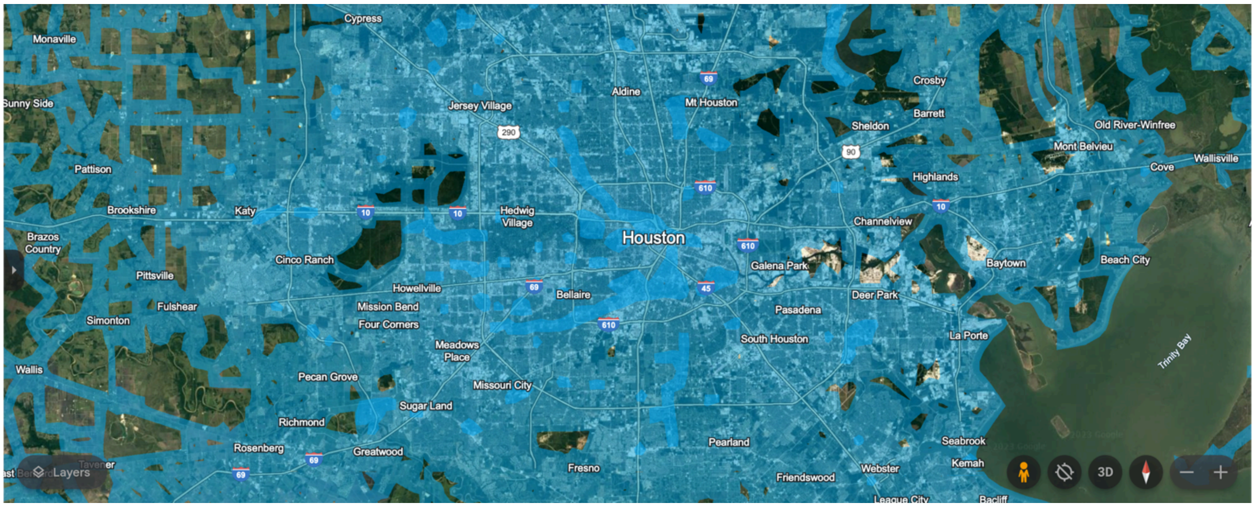


Figure 5: Houston, Texas. The areas in blue have been imaged by Google Street View © Google Earth

3.2 Camera Analysis

It is purposefully difficult to find the exact model of camera that police departments use and the model of private cameras is almost never publicly available so we plan to generalize out the Argus camera modeling used by Amnesty International which suggests have the capacity to track faces from as far as 200 meters away (or up to 2 blocks) [27]. We believe that this modeling is appropriate to extrapolate because even if other municipalities have less capable cameras, the use case of the platform lends itself to the overestimation of surveillance.

3.3 Modeling Threats to Reduce Risk

Amnesty International produced mitigation strategies to tease out discrete risks involved with the scope and methodology of the project that will be adopted for our model [38].

When completing tasks, volunteers are unsure which cameras are public.	● Create a Help section in the task presenter ● User demo ● Review the level of "agreement" between decoders
When completing tasks, volunteers at different locations count the same camera causing duplicates in the data.	● Limit zoom and user test ● Account for the scenario in the onboarding tutorial and user test ● When post-processing the data, use the proximity of locations, camera classification, and/or URLs/hashes to identify duplicates in the data
Volunteers do not agree on the number of cameras.	● Completion criterion is the number of submissions. The level of agreement does not affect completion.

Volunteers do not reliably categorize camera types, meaning it takes more users than expected to meet the matching criteria.	● Camera categorization does not determine the completion criteria. ● Have a category that is "Don't know or other camera type"

3.4 Micro-tasking Design

It is important for the research to be able to classify cameras as publicly or privately owned. Without access to this information and to keep the micro-tasking questions as simple as possible, the team decided to use what cameras were attached to as a proxy for public or private ownership.

Participants were asked to find all surveillance cameras and record what they were attached to. Three multiple-choice options were given:

- Streetlight, traffic signal or pole
- Building
- Something else

If participants selected Option 1. "Streetlight, traffic signal or pole", they were asked to identify the camera type. We chose three visually distinct, high-level categories:

- Dome or PTZ camera[1]
- Bullet camera
- Unknown or Other

The answers were then used as a proxy for public or private ownership. For example, cameras attached to traffic signals or streetlights were assumed to be most likely owned by a government agency. In this sub-category, dome or PTZ cameras were of particular interest as they were likely to be NYPD Argus cameras. Whereas cameras attached to buildings were assumed to be privately owned and so of less relevance to the research, although we recognized that a minority would be attached to federal buildings.

[1] PTZ is an acronym for Pan Tilt Zoom

While this methodology worked in New York, we have a hesitancy to generalize it out to other municipalities given that they may not utilize the same type of cameras. We plan to utilize this tagging model until we have a significant number of tags wherein if we find a disproportionate level of "Something else" location tags or "Unknown or Other" camera tags we will redevelop the micro-tasking design. This is why for the preliminary tagging stages in non-New York cities, we will also implement a comment feature in the tagging model wherein participants can add comments or notes if they encounter unique situations or challenges. We will utilize these qualitative insights to better understand the context of certain findings and fine-tune the micro-tasking model. This step will also provide valuable tagging data for our deep vision model.

3.5 Support and Accessibility

Decoders demonstrated that the quality of the data collected rested on consistent answers and a function for taggers to agree with each other the majority of the time [38]. The multiple-choice questions were illustrated by pictograms drawn by an illustrator. The illustrations were used throughout the project site to reinforce instructions and as visual aids for volunteers who were not fluent in English or would otherwise benefit.

Amnesty International implemented a moderated forum where participants could access the forum via the navigation bar at the top of the page or by flagging the task for discussion [34]. Flagging an assignment opened a new discussion thread if the traffic intersection had not been flagged before or added to an existing in the forum and participants could add a comment/question and upload supporting materials such as screenshots and links.

As an organizer-forward platform, we plan to create a forum feature that is integral to app usage. Centered around city-based discussion boards and tagging groups. As well as "legacy contribution" mechanisms to ensure user safety within a pseudo-anonymous platform wherein users with app longevity and proven benevolent intent not only have a more valued tagging input but also the ability to moderate the discussion.

3.6 Other Key Platform Components

The goal of Watch the Watchers is to increase public consciousness of surveillance which we believe cannot be done without collaboration.

3.6.1 Mechanisms for User Privacy

User privacy is a chief priority for a platform where the protection of civil liberties is the priority. There is a demonstrated intent to dismantle the right to organize especially in online spaces [11]. This is why we plan to create and develop distinct storage systems for tagging data and communication data to minimize the risk of unintended access. And develop a mechanism to protect private communications from public components ensuring that sensitive or private communications between volunteers are secure and not accessible by the general public. The implementation of end-to-end encryption (E2EE) for all private communications access to facilitate secure and private direct messaging between participants [42], similar to popular secure messaging apps like Signal [43].

The forum and messaging spaces allow users to employ end-to-end encryption for direct messaging to safeguard message content, allow for self-destructing messages or message expiration options to enhance privacy, and use a user-friendly and accessible interface. These features collectively aim to establish a robust and secure framework for data collection, communication, and retention within the surveillance camera tagging application. This is all in tandem with robust data storage and retention practices that will not collect excess biographic information about users and routinely erase user communications at a period set by the individual user.

Yadav et al. developed a user-controlled application-independent encryption model in 2023, *InfoGuard* [42], that we plan to integrate as the basis for the E2EE encryption of Watch^2. *InfoGuard* allows users to trigger encryption on any textbox, even if the application does not support E2EE. *InfoGuard* encrypts text before it reaches the application, eliminating the Watch^2 access to plaintext. *InfoGaurd* also incorporates visible encryption to make it easier for users to understand that their data is being encrypted and give them greater confidence in the system's security. The design enables fine-grained encryption, allowing specific sensitive data items to be encrypted while the rest remains visible to the server. *InfoGaurd* also compensates for the encryption adversary, *A*, which is an active global attacker that controls an application server with plaintext access to all messages and metadata flowing through it [42]. This is a highly plausible scenario as there is the precedent of law enforcement attempting to access secure messaging even E2EE messaging of organizers [15]. Law enforcement concerns sometimes lead to discussions about banning E2EE. Instead of an all-or-nothing approach, *InfoGuard* is a middle-of-the-road solution that allows a user to send a message and encrypt only the most sensitive data (e.g. account numbers, SSNs, currency totals) [42]. It allows auditors to view the purpose and non-sensitive data in the message while safeguarding sensitive data.

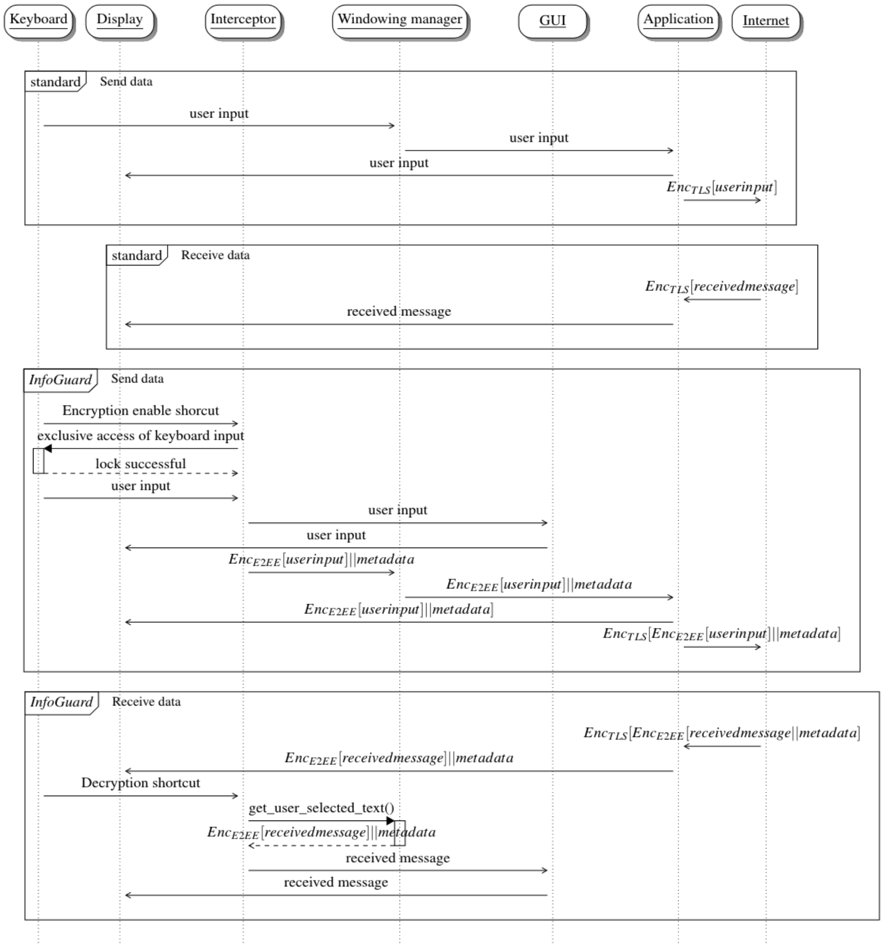
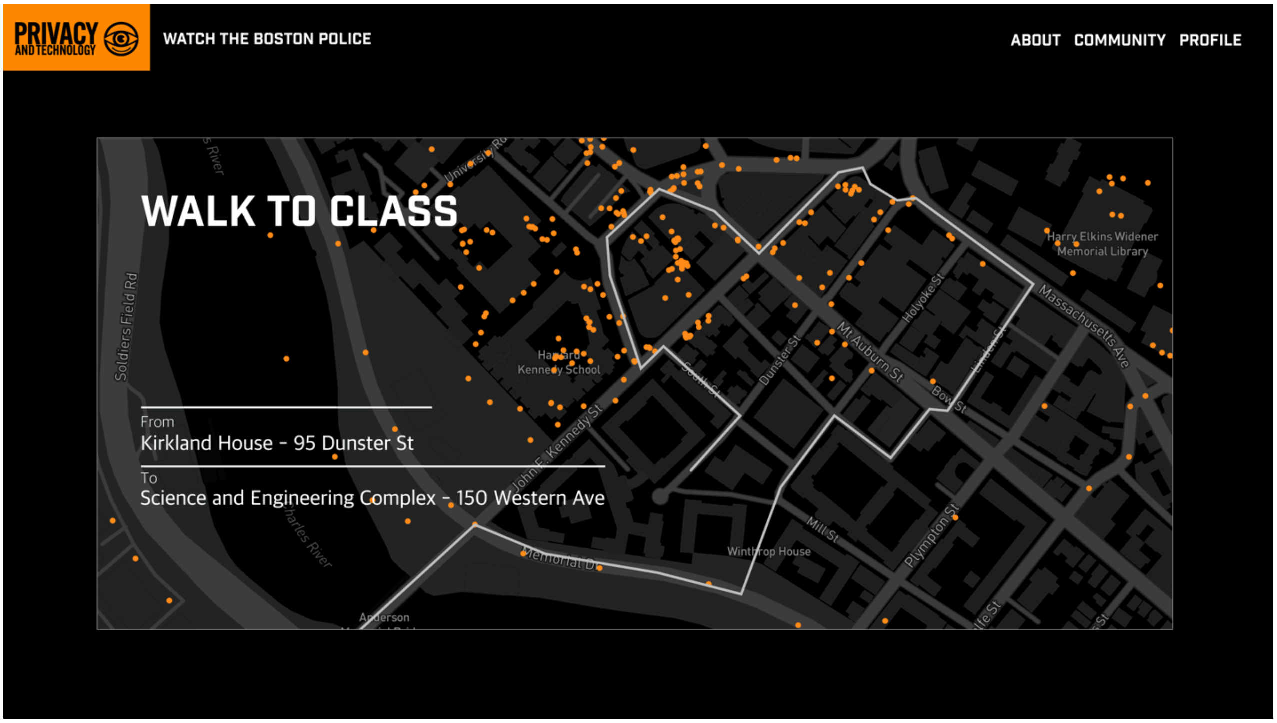

Keyboard
Display
Interceptor
Windowing manager
GUI
Application
Internet
standard
Send data
user input
user input
user input
$Enc_{TLS}[userinput]$
standard
Receive data
$Enc_{TLS}[receivedmessage]$
received message
InfoGuard
Send data
Encryption enable shorcut
exclusive access of keyboard input
lock successful
user input
user input
user input
$Enc_{E2EE}[userinput]||metadata$
$Enc_{E2EE}[userinput]||metadata$
$Enc_{E2EE}[userinput]||metadata]$
$Enc_{TLS}[Enc_{E2EE}[userinput]||metadata]$
InfoGuard
Receive data
$Enc_{TLS}[Enc_{E2EE}[receivedmessage||metadata]$
$Enc_{E2EE}[receivedmessage]||metadata$
Decryption shortcut
get_user_selected_text()
$Enc_{E2EE}[receivedmessage]||metadata$
received message
received message

Figure 7: InfoGuard message flow. Note, messages from the application/GUI to display are directly transmitted in this diagram for simplicity. In reality, messages to display are transmitted through the windowing manager [42].

3.6.2 Exposure-Based Navigation System

The key component of Watch the Watchers will be the camera exposure-based navigation system. Participants will be able to input an origin and destination point in any of our target cities on Watch[2]. We will integrate the collected data on surveillance cameras into the navigation system, creating a comprehensive database of camera locations and developing algorithms that analyze camera density, types, and other relevant factors to generate routes with varying levels of camera exposure. Just like map navigation algorithms rely on shortest path algorithms like the Dijkstra's Algorithm and A* Algorithms [44] our platform will:

- allow users to view how exposed these paths are,
- find the tradeoff between the shortest path and least exposure, and
- apply these features to plan protest routes with specific points of interest that will either:
  - avoid the maximum number of cameras, and/or
  - give organizers a clear picture of how their movements are being captured by physical surveillance infrastructure.



From
Kirkland House - 95 Dunster St

To
Science and Engineering Complex - 150 Western Ave

Figure 8: Mockup of Navigation Panel for Daily Route from Cambridge, MA to Allston, MA

4. PREDICTED EVENTS

This literature review has outlined the demonstrated need for a change in our country's surveillance system or, at the very least, our relationship with this system. The desired outcome for our platform involves the development of a robust technological framework that empowers individuals from unawareness about government surveillance and protects them from the detrimental effects of over surveillance. This technology should act as a safeguard against malicious uses of surveillance, particularly regarding physical camera infrastructure and facial recognition.

Construct: A Crowdsourced Camera Tagging Platform identifies cameras in major metropolitan areas, navigate based upon camera exposure, and internally communicate.

Such that: Individuals can confidently privately accurately identify camera location and type, thereby creating an accurate database for the navigation algorithm. This system should be user-friendly, accessible, and continuously updated to adapt to the changing surveillance infrastructure. Internal direct communication should also be end-to-end encrypted to the level that passive and active adversarial attempts to access messaging are unsuccessful. The overarching goal is to increase the public consciousness of surveillance in American cities and instill a sense of security and trust in digital communications.

4.1 Evaluation

Below is the set of metrics we will use to evaluate the application;

4.1.1 Tagging Accuracy

Tagging accuracy is central to the integrity of Watch^2. Therefore, it is crucial to develop a method to test tagging accuracy. This can be done by having every new participant evaluate a set of pre-tagged intersections wherein researchers have definitively tagged the correct locations and models of every camera in the intersections. This will serve as a baseline to gauge the contribution/intent of new platform participants.

4.1.2 Tagging Agreement

As mentioned in 2.1, Amnesty International excluded the use of Krippendorff's alpha (α), a method to counteract tagging disagreement in their original study.

Our potential model for Krippendorff's Alpha exists wherein *n* number of observers can select from three base options: 1. Streetlight, traffic signal, or pole/2. Building/3. Something else, and if participants selected Option 1. "Streetlight, traffic signal or pole", they were asked to identify the camera type. there's an additional three distinct, high-level categories: Dome or PTZ camera/Bullet camera/Unknown or Other.

The number of observers is denoted as n, the number of base options (3) as, and the number of categories within each option (3) as *C*.

Each observer will rate each unit, and Options 2 and 3 will always have 0 as their secondary denotation since. The values assigned by the observers could be represented by a matrix *O* where O_{ij} is the rating given by the *i*-th observer to the *j*-th unit.

Now, let's denote N_{uc} as the number of times category *c* is assigned to unit u, and N_{kc} as the number of times category *c* is assigned by observer *k*. The total number of observations is $N = n \times U$

To calculate Krippendorff's Alpha, we need to compute two terms: D_o (observed disagreement) and D_e (expected disagreement). See section 2.1 for a more detailed explanation of disagreement coefficients.

$$D_o = \frac{1}{N} \sum_{u=1}^{U} \sum_{v=1}^{U} \sum_{c=1}^{C} N_{uc} \left(N_{vc} - \delta(u, v) \right)]$$

$$D_e = \frac{1}{(N-1)} \sum_{k=1}^{n} \sum_{u=1}^{U} \sum_{v=1}^{U} \sum_{c=1}^{C} N_{kc} \left(N_{kc} - \delta(u, v) \right)$$

Here, *δ(u,v)* is the Kronecker delta function (1 if u=v, 0 otherwise).

Finally, Krippendorff's Alpha (α) is calculated using the formula:

$$\alpha = 1 - \frac{D_o}{D_e}$$

This model considers the disagreement and agreement among observers regarding the assigned categories to different units. The calculation involves comparing the observed disagreement to the expected disagreement between participants about both camera location and type, providing a measure of inter-coder reliability.

Since this model is still new and their development and application to this type of data is so recent this would be an amazing use case to test their application in this field, but we may not yet have enough experience in interpreting and using them. It may be more economical to use a more traditional comparison method like Analysis of Variance (ANOVA).

4.1.3 Navigation Optimization

As mentioned in 3.6.2, a key feature of Watch^2 is its camera-exposure-based navigation system. Developing a system that allows users to decide their individual trade-offs; exposure or efficiency, will be crucial to gauging the app's success.

4.1.4 Message Encryption Security

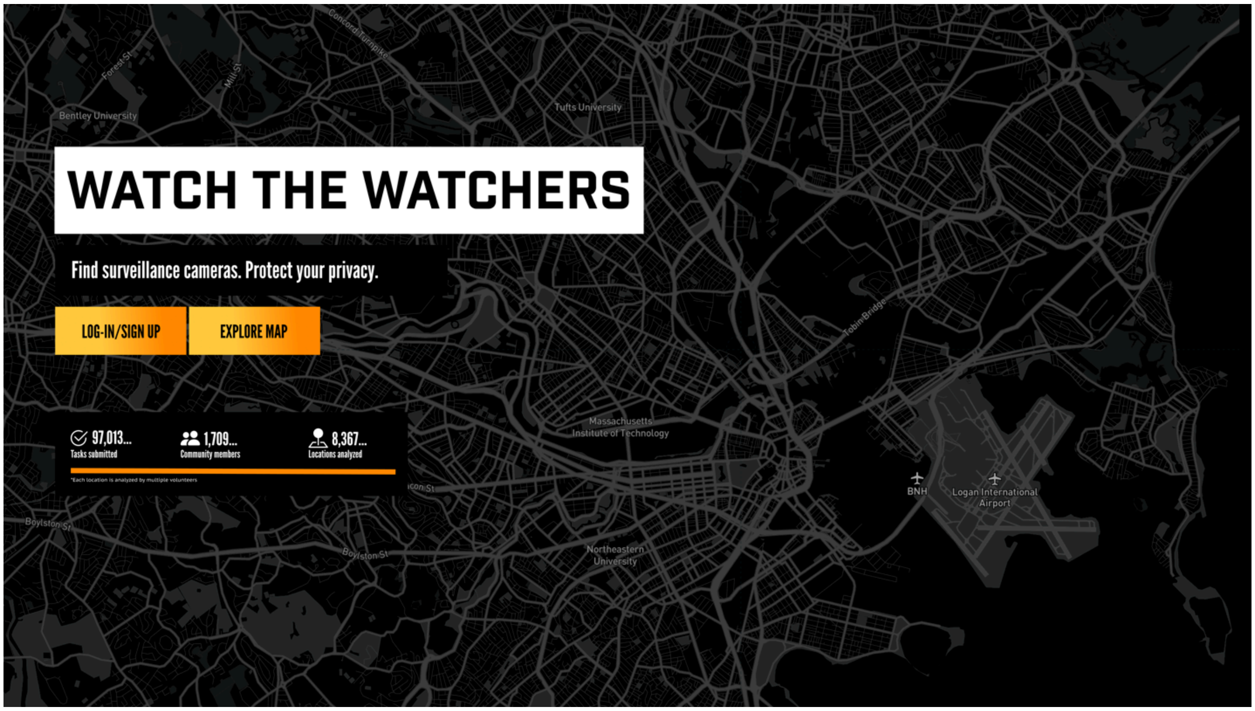
The usually app-based E2EE mechanism is susceptible to two types of client-side attacks: passive and active [42]. Passive attacks involve reading user text while they type in the app and sending it to the server or having bugs that allow other attackers to access plain text passively. Active attacks involve the client app actively attempting to access the plaintext, even when the user does not enter it directly into the app. None of the standard app-based E2EE protocols prevent these attacks. *InfoGuard* prevents plaintext access even against active attacks by intercepting and encrypting key presses before passing them to the windowing manager. So a test must be done to test the efficacy of this mechanism in Watch the Watchers.

5. DISCUSSION

Individual solutions like facial recognition deterrence do nothing to address the problem of over surveillance, especially in cities where facial recognition has already been banned and policy solutions like regulation and oversight get stonewalled by government bureaucracy.

Our intention is for this paper to serve as the framework for a platform that will equip citizens with the tools to control their piece of mind. We understand that the methods in this paper are untested and are eager to find the opportunity to develop the project into its beta phase.

We acknowledge that the initial framework for our project is based largely on Amnesty International's Decoders model. Amnesty has invited the replication of their data and methodology, but this is only a launching point for a more permanent platform. The secondary goal of Watch the Watchers is to see if the results in New York can be replicated in other cities because the right to assemble is not just being infringed upon in New York. We plan for Watch the Watchers to serve as a tool of empowerment for non-academics and non-New Yorkers because every citizen deserves the ability to understand when, where, and how they're being watched.



WATCH THE WATCHERS

Find surveillance cameras. Protect your privacy.

97,013... Tasks submitted

1,709... Community members

8,367... Locations analyzed

*Each location is analyzed by multiple volunteers

Figure 9: Watch the Watchers Desktop Homepage Mockup

6. REFERENCES

[1] "International Covenant on Civil and Political Rights," OHCHR. Accessed: Dec. 04, 2023. [Online]. Available: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[2] M. Foucault, "'Panopticism' from 'Discipline & Punish: The Birth of the Prison,'" *RaceEthnicity Multidiscip. Glob. Contexts*, vol. 2, no. 1, pp. 1–12, 2008.

[3] "Inside the NYPD's Surveillance Machine." Accessed: Nov. 28, 2023. [Online]. Available: https://banthescan.amnesty.org/decode/

[4] "Police surveillance in New York City," *Wikipedia*. Jan. 18, 2023. Accessed: Nov. 11, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Police_surveillance_in_New_York_City&oldid=1134360529

[5] Sidney Fussell, "The NYPD Had a Secret Fund for Surveillance Tools," *WIRED*, Aug. 10, 2021. Accessed: Nov. 15, 2023. [Online]. Available: https://www.wired.com/story/nypd-secret-fund-surveillance-tools/

[6] C. Worthington, "Safety as a Smokescreen: The New York Police Department, Surveillance Technology, and Necropower," Columbia University, 2022. doi: 10.7916/8s24-dv58.

[7] City of Boston, "Boston's Use of Surveillance Technology." Accessed: Nov. 25, 2023. [Online]. Available: https://www.boston.gov/bostons-use-surveillance-technology

[8] Privacy SOS, "'See Something, Say Something' -- unless it's omnipresent government surveillance," Privacy SOS. Accessed: Nov. 25, 2023. [Online]. Available: https://privacysos.org/blog/see-something-say-something-unless-its-omnipresent-government-surveillance/

[9] J. A. Hendrix, T. A. Taniguchi, K. J. Strom, K. A. Barrick, and N. J. Johnson, "The Eyes of Law Enforcement in the New Panopticon: Police-Community Racial Asymmetry and the Use of Surveillance Technology," *Surveill. Soc.*, vol. 16, no. 1, pp. 53–68, Apr. 2018, doi: 10.24908/ss.v16i1.6709.

[10] C. Sheridan, "Foucault, Power and the Modern Panopticon".

[11] D. Murray *et al.*, "The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe," *J. Hum. Rights Pract.*, p. huad020, Jul. 2023, doi: 10.1093/jhuman/huad020.

[12] F. Chideya and C. Turner, "COINTELPRO and the History of Domestic Spying," *NPR*, Jan. 18, 2006. Accessed: Dec. 16, 2023. [Online]. Available: https://www.npr.org/templates/story/story.php?storyId=5161811

[13] Paul Wolf, "COINTELPRO: The Untold American Story," U.N. High Commissioner for Human Rights, World Conference Against Racism in Durban, South Africa, Sep. 2001. Accessed: Dec. 16, 2023. [Online]. Available: https://cldc.org/wp-content/uploads/2011/12/COINTELPRO.pdf

[14] "Post-9/11 surveillance has left a generation of Muslim Americans in a shadow of distrust and fear | PBS NewsHour." Accessed: Dec. 16, 2023. [Online]. Available: https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear

[15] E. Goitein, "Rolling Back the Post-9/11 Surveillance State," Brennan Center for Justice. Accessed: Dec. 16, 2023. [Online]. Available: https://www.brennancenter.org/our-work/analysis-opinion/rolling-back-post-911-surveillance-state

[16] "NYPD's Legacy Of Police Surveillance, From Black Panthers To Mosques To Black Lives Matter - Gothamist." Accessed: Dec. 16, 2023. [Online]. Available: https://gothamist.com/news/nypds-legacy-of-police-surveillance-from-black-panthers-to-mosques-to-black-lives-matter

[17] E. Heh and J. Wainwright, "No privacy, no peace: Urban surveillance and the movement for Black lives," *J. Race Ethn. City*, vol. 3, no. 2, pp. 121–141, Jul. 2022, doi: 10.1080/26884674.2022.2061392.

[18] E. Honstein, "Protesting in an Age of Government Surveillance," ICNL. Accessed: Nov. 15, 2023. [Online]. Available: https://www.icnl.org/post/analysis/protesting-in-an-age-of-government-surveillance

[19] B. X. Chen, "Security Cameras Make Us Feel Safe, but Are They Worth the Invasion?," *The New York Times*, Nov. 02, 2022. Accessed: Dec. 04, 2023. [Online]. Available:

https://www.nytimes.com/2022/11/02/technology/personaltech/security-cameras-surveillance-privacy.html

[20] M. E. Kaminski and S. Witnov, “The Conforming Effect: First Amendment Implications of Surveillance, beyond Chilling Speech,” *Univ. Richmond Law Rev.*, vol. 49, no. 2, pp. 465–518, 2015 2014.

[21] M. Nkonde, “Automated Anti-Blackness: Facial Recognition in Brooklyn, New York”.

[22] J. A. Buolamwini, “Gender shades : intersectional phenotypic and demographic evaluation of face datasets and gender classifiers,” Thesis, Massachusetts Institute of Technology, 2017. Accessed: Dec. 16, 2023. [Online]. Available: https://dspace.mit.edu/handle/1721.1/114068

[23] K. Crockford, “How is Face Recognition Surveillance Technology Racist? | ACLU,” American Civil Liberties Union. Accessed: Dec. 16, 2023. [Online]. Available: https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist

[24] T. L. Johnson, N. N. Johnson, D. McCurdy, and M. S. Olajide, “Facial recognition systems in policing and racial disparities in arrests,” *Gov. Inf. Q.*, vol. 39, no. 4, p. 101753, Oct. 2022, doi: 10.1016/j.giq.2022.101753.

[25] “Phoenix PD called protesters ‘targets’ during surveillance, before arrests.” Accessed: Dec. 16, 2023. [Online]. Available: https://www.abc15.com/news/local-news/investigations/protest-arrests/phoenix-police-called-protesters-targets-during-surveillance-before-arrests

[26] Amnesty International, “Ban facial recognition technology,” Amnesty International. Accessed: Nov. 15, 2023. [Online]. Available: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

[27] “New York is in danger of becoming a total surveillance city,” Amnesty International. Accessed: Nov. 30, 2023. [Online]. Available: https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/

[28] Tate Ryan-Mosley, “The NYPD used a controversial facial recognition tool. Here’s what you need to know.,” *MIT Technology Review*, Apr. 09, 2021. Accessed: Dec. 16, 2023.

[Online]. Available: https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/

[29] B. Lambert, “Secret Surveillance Cameras Growing in City, Report Says,” *The New York Times*, Dec. 13, 1998. Accessed: Dec. 16, 2023. [Online]. Available: https://www.nytimes.com/1998/12/13/nyregion/secret-surveillance-cameras-growing-in-city-report-says.html

[30] L. Siegel, Robert A. Perry, and Margaret Hunt Gram, “Who’s Watching? Video Camera Surveillance in New York City and the Need for Public Oversight,” *N. Y. Civ. Lib. Union*.

[31] New York Surveillance Camera Players, “Maps of Publicly Installed Surveillance Cameras in New York City,” Not Bored. Accessed: Dec. 16, 2023. [Online]. Available: https://www.notbored.org/scp-maps.html

[32] New York Surveillance Camera Players, “A Guide to Mapping Surveillance Cameras,” Not Bored. Accessed: Dec. 16, 2023. [Online]. Available: https://www.notbored.org/map-making.html

[33] New York Surveillance Camera Players, “A Guide to Surveillance Cameras.” Accessed: Dec. 16, 2023. [Online]. Available: https://www.notbored.org/camera-types.jpg

[34] Amnesty International, “Decode Surveillance NYC.” Accessed: Nov. 25, 2023. [Online]. Available: https://decoders.amnesty.org

[35] Amnesty International, “NYPD ordered to hand over documents detailing surveillance of Black Lives Matter protests following lawsuit,” Amnesty International, New York, N.Y., Aug. 2022. Accessed: Dec. 16, 2023. [Online]. Available: https://www.amnesty.org/en/latest/news/2022/08/usa-nypd-black-lives-matter-protests-surveilliance/

[36] B. Hamilton, “HIDDEN EYES OF OUR APPLE ; NO ESCAPING CITY SECURITY CAMERAS,” *New York Post*, May 02, 2004. Accessed: Dec. 16, 2023. [Online]. Available: https://nypost.com/2004/05/02/hidden-eyes-of-our-apple-no-escaping-city-security-cameras/

[37] K. Krippendorff, “Computing Krippendorff’s Alpha-Reliability”.

[38] Amnesty International, “Decode Surveillance NYC Methodology Report,” Amnesty International, New York, NY, 2021. Accessed: Nov. 28, 2023. [Online]. Available: https://banthescan.amnesty.org/wp-content/uploads/2022/02/AMR5152052022EN_DecodeSurveillanceNYCMethodology.pdf

[39] Y. Zhang *et al.*, "Recognize Anything: A Strong Image Tagging Model." arXiv, Jun. 09, 2023. doi: 10.48550/arXiv.2306.03514.

[40] Google, "Google-Contributed Street View Imagery Policy," Google Maps Street View. Accessed: Dec. 16, 2023. [Online]. Available: https://www.google.com/streetview/policy/

[41] Google, "Google Earth." Accessed: Dec. 16, 2023. [Online]. Available: https://earth.google.com

[42] T. Yadav, A. Cook, J. Hales, and K. Seamons, "InfoGuard: A Design and Usability Study of User-Controlled Application-Independent Encryption for Privacy-Conscious Users." arXiv, Nov. 01, 2023. doi: 10.48550/arXiv.2311.00812.

[43] "Signal Messenger: Speak Freely," Signal Messenger. Accessed: Dec. 17, 2023. [Online]. Available: https://signal.org/

[44] D. Rachmawati and L. Gustin, "Analysis of Dijkstra's Algorithm and A* Algorithm in Shortest Path Problem," *J. Phys. Conf. Ser.*, vol. 1566, no. 1, p. 012061, Jun. 2020, doi: 10.1088/1742-6596/1566/1/012061.