# Implementing and Communicating Privacy by Design in CCTV Cameras

Drew Callahan
University of Chicago
1100 E 58th St
Chicago, Illinois
xxx@uchicago.edu

Mike Gu
University of Chicago
1100 E 58th St
Chicago, Illinois
xxx@uchicago.edu

Jesse Martinez
University of Chicago
1100 E 58th St
Chicago, Illinois
xxx@uchicago.edu

Lefan Zhang
University of Chicago
1100 E 58th St
Chicago, Illinois
xxx@uchicago.edu

## ABSTRACT

The rapid development of the Internet of Things (IoT) and the increased use of IoT devices in urban environments has produced a number of unanswered questions regarding the privacy of the people in these settings. Notably, there is a discrepancy between the capacity of urban IoT devices and of standard smart devices to communicate information about privacy: a smartphone can display text explaining the details of a privacy policy, but a smart traffic camera without a screen has little capacity to inform a passing car of what data it is gathering. Arguably, it is even more important that sensors in urban environments communicate their privacy policies, as they cannot necessarily assume the same level of consent that a smartphone can assume of its user. In an attempt to address some of these questions, we conducted a survey to explore people's opinions of the privacy protectiveness or invasiveness of urban IoT devices, and used this information to conduct a lab study in which we attempted to identify whether the way in which a device attempted to communicate its privacy protective features affected participants' awareness of these features, as well as the degree to which participants were comfortable with or trusted the device. We found that the choice of display channel did affect user perceptions, and that some channels were more effective at communicating this information than others.

## 1. INTRODUCTION

The Internet of Things is increasingly changing the world of business, industry, and daily life. Network connected sensor devices have driven new efficiencies and innovations in a variety of sectors and have shown no signs of stopping. The total number of IoT connections is poised to increase fourfold by 2020. With this massive growth in data connectivity comes numerous issues regarding privacy and security. New vulnerabilities in data infrastructure will inevitably be exploited, which is why privacy by design is so crucial. In order for the IoT and the devices associated with it to maintain consumer and governmental confidence, the concept of privacy by design must be made obvious in the public sector. Our contribution is be two-fold. First, we explored the design space of privacy protection notification for urban sensors. This is fundamentally challenging, because normally sensors don't provide any interface that can actively communicate with users. For that reason, common methods of communicating privacy, such as pop-up permission notifications (like those on smart phones or PCs), don't apply to urban sensors. This highly limits the design space for notification for privacy policy. Another challenge is the urban location of the sensor, whether they are mounted thirty feet up or easily accessible at ground level. Whether they are surrounded by hazards such as cars, or immersed in water. How easily the sensor is publicly viewable or audibly noticeable affects the design of the privacy notification. What is also challenging is the communication of nuanced IoT security protocols, such as the type of encryption, the node security, how the data is stored etc. Visual design and appeal is also an entirely other dimension to explore. These numerous confounds and more comprise the design space of urban sensors.

### 1.1 Data display

We primarily chose to focus on four fundamental types of communicative displays that will likely apply to a wide range of IoT applications: video footage, audio, LED's, and static text. These display modes were based off the 'modalities' of privacy notifications proposed by Schaub et al. The goal of was to engage in an exploratory analysis of how these different modes of display impact an individual's privacy/comfort as well as two new factors of trustworthiness and clarity of information. As this is an exploratory analysis we feel this wide range approach will be effective at narrowing down in the future iterations the type of medium that should be used to create a usable and informative display. Using an interview-based study, we examined the responses of the individuals to determine if any of the proposed modes should be looked into more in a future iteration of the study focus-


*USENIX Symposium on Usable Privacy and Security (SOUPS)* 2018.
August 12–14, 2018, Baltimore, MD, USA.

ing on variations of that mode.

## 1.2 Data collection

To measure the effectiveness of these different displays we designed a lab study where participants interacted with a privacy display notification for a camera. We subsequently interviewed about them about their general comfort with the camera, as well as their perceptions of who can access the data, what data can be accessed, and how long the data can be accessed. We judged the accuracy of their answers to represent the effectiveness of the privacy notification. These three factors, "who", "what", and "how long", were inspired by Hosub Lee's and Alfred Kobsa's previous work developing five contextual parameters that characterize privacy preferences towards IoT service scenarios [13]. These five contextual parameters included place ("where"), type of collected information ("what"), agent ("who"), purpose ("reason") and frequency ("persistence") of the monitoring. They found all of these contextual parameters, with the exception of "persistence", to have a strong effect on how accepting the user was of each scenario. Although Lee and Kobsa's work was extremely comprehensive in encapsulating privacy preferences in IoT scenarios, they acknowledged that their study lacked ecological validity, given that it was an online survey. Our work is unique in that we are exploring these privacy preferences in the context of a field study with a real, live-processing device in front of the participants and that we included an additional element of data storage that Lee and Kobsa neglected.

## 1.3 Initial Hypothesis & Research Questions

In the data collection phase we expected to discover that:

- Each factor is significant
- There is some interaction effect between the factors
- These factors can be realistically altered to significantly reduce the invasion of privacy

In the data display phase we expected to discover that:

- All four modes are viable approaches
- An ordinal scale of video>LEDs>audio>text can be formed from the coding
- Text will not require further study
- Audio given the difficulty with ambient noise drowing it out will not acquire positive enough results to warrant a more in-depth study
- LEDs will be an effective approach relative text and will most likely require further study into color, quantity, etc.
- Display will be an effect approach relative to text and will most likely require further study in the best manner to present broad types of filtered data

# 2. BACKGROUND & RELATED WORK

## 2.1 Privacy by design and privacy notifications

Privacy has been people's concern for a long time. In traditional scenarios, privacy is protected by regulations, laws and practices. However, with a higher concentration of information-gathering technologies in everyday life, an engineering effort needs to be taken to provide better privacy experience for users; this has led to the conclusion that privacy should be considered in design stage, establishing the concept of "privacy by design" [18]. Multiple studies have explored the expectations of privacy design as well as the design space of the issue [18, 10], proposing design principles and guidelines. Spiekermann et al. summarized users' privacy concerns and mapped them to three system operations: data transfer, storage, and processing [18]. In this work, approaches to provide privacy, "privacy by policy" and "privacy by architecture", were discussed [18]. GÃijrses et al. implemented two case studies in privacy engineering, and showed that data minimization could be the principle behind privacy design of systems [10].

The development of techniques to protect privacy is not the end of the road. Users should be informed about their privacy protection status, understand privacy issues, and make choices about privacy policy as well. However, current work shows that there might be some gap between privacy design in systems and users' understanding of it. Recent studies have focused on how to design effective privacy notifications. Schaub et al. explored the design space for privacy notices [16]. According to their study, privacy notices can differ in timing, channel (i.e. interface where notices are conveyed), modality (visual, auditory, etc.) and control (whether users need to confirm the notice to continue), which could all influence the effectiveness of notices [16]. Several studies focused on specific privacy notifications. For example, the design (shape, color) of icons shown in Internet browsers to indicate whether a connection is secure may differ in effectiveness [6]. Moreover, Gluck et al. studied the influence of notifications' length and framing on their effectiveness, concluding the length of a notification's text had a larger influence on its effectiveness than its framing [8]. However, previous studies focus a lot on devices with ample interface to interact with users such as smartphones and computers. Less work has been done on those devices without such an interface, especially Internet of Things (IoT) devices and sensors in urban environments. Design space on privacy notifications for such devices need to be studied in order to provide users with better understanding on the devices' privacy protection design.

## 2.2 IoT privacy

Researchers have conducted several studies relating to the Internet of Things and privacy. There is much work to be done in not only communicating privacy and trust surrounding IoT but also in establishing a common groundwork of IoT itself such that privacy is built into its fundamental design. This is difficult because there is so much variation between IoT devices, ie: the bandwidth used, the type of data that is collected, etc. Too many standards of communication stacks are involved which makes regulating security and privacy for IoT a frustrating endeavor. There is research being done on a trust system involving mutual feedback on nodes [17], but before there is a common system

established, we would not be able to reference any universal symbols or frameworks involving IoT to build an effective communication system for this project. With regard to users themselves, researchers have found that privacy preferences are highly context dependent. Hosub Lee and Alfred Kobsa managed to categorize these preferences under five contextual parameters: "place ("where"), type of collected information ("what"), agent ("who"), purpose ("reason") and frequency ("persistence") of the monitoring" through a survey [13]. We are interested particularly in measuring these contextual parameters through a usability test with special regard to how long the data is stored and how the method of display affects communication of these parameters. We also contacted the Array of Things team for a brief conversation on the measures they took to communicate IoT privacy by design. Essentially, they prioritized branding and visual appeal, even contacting the institute of fine arts for design advice, with the goal that security of data could be communicated through brand strength. They did this for a variety of reasons, foremost being that their sensors are mounted too high up for privacy displays on the sensors themselves to be practical for public viewing. When asked about publicly accessible privacy displays, they mentioned an Australian security camera example where an interactive touch screen with information about the camera was positioned below the camera. This display design was the basis of our experiment setup - a camera and a corresponding display notification positioned next to the camera.

## 2.3 IoT in ubiquitous computing environments

A common theme in the existing literature on IoT in urban environments is the difficulty in handling the heterogeneous make up of sensory devices and the best architecture to collect this information into a single easily accessible location.

Gaur et al. discuss this by breaking the "Smart City" into several components that come together to form it [7]. Their strategy is to break up this process into 4 steps. These 4 steps are collecting the information, parsing it into a common format, integrating this data, and then making the data accessible by some query language. Their model seeks to empower users to better understand the environment around them, while doing most of the analysis within the system and outside applications.

Similarly, Li Da Xu et al. also discuss a method for developing the architecture of the IoT devices [3]. They discuss a 4-layer architecture that fundamentally breaks down to a similar process of collecting heterogeneous information and making it available to users. However, they chose to place the brunt of handling the heterogeneity and analysis on the application. Due to this choice of making raw data available to applications, they discuss the need for encrypting the collected information. Furthermore, they seek to integrate the sensory information with the cloud and social media, with the aim of improving data aggregation. This further complicates the scope of the information collected as well the necessary precautions required.

Gomez et al. describe another architecture level [9]. This architecture aims to have the sensors locally process data and then send this data to listening sensors which will then forward it to requesting servers. This architecture mirrors the Gaur et al. paper, in that a lot of the analysis is done on the sensor, but the analysis is not standardized and collected into a central hub. This architecture still requires the application to handle the heterogeneity of the analyzed information requiring further raw information to be passed to the application.

Rathore et al. propose a similar architecture to Gaur et al [15]. They desire to implement a 4-layer architecture that mirrors current Internet standards. Their system is more involved than the previous architectures as they seek to provide a filtering method to handle the heterogeneous information and separate into categories [15]. Then this data will be pre-processed and then analyzed to make adjustments to the smart city. This system has like the first completely analyzed the data into a standard format requiring little extra information to be passed onto applications to make sense of the data collected. As such they have a more fleshed out central hub that contains the standardized and filtered information, which can then be further processed by the application.

Bates, et. al. discuss the actual implementation of IoT within a university setting [1]. The results from this venture found that a decently complex system could be created by linking existing sensors and aggregating this information into a single hub. This provided some of the data driven optimization that other papers had discussed as possibilities. The main purpose of the paper was to discover certain underlying difficulties in creating the system. These manifested mostly in difficulties with handling existing sensors and connecting them to the IoT system. There were as well difficulties with handling the dissemination of collected information. The paper discusses the flaws around the system being an incomplete data hub, requiring further integration of more sensors to collect more information and at a higher granularity, to better provide the desired information dissemination level.

All of these papers discuss the difficulties in implementing either in theory or in practice a "smart city". The main issues that every paper found was how to handle the heterogeneous makeup of information and how best to provide this information to users. The approaches for dealing with the heterogeneity of the data are handling it on some level of the architecture, which will also vary depending on the IoT system. As a result, the state of the data could either be processed or raw at any point depending on the architecture of the system. The results of the papers show that the privacy of individuals will vary within any IoT system and furthermore will vary among IoT systems. While there is a strong push for a standardized architecture, this is most likely infeasible. The result will be that several cities choose their own architecture to enable their IoT "Smart City". Furthermore, within any of these architectures the sensors used will also vary greatly. Due to this variation at all levels of the IoT system, any static approach to usability would be too specific to enable general use of the conclusions brought from the study. Therefore, a dynamic approach to usability is required to accommodate this variation between and within IoT systems, including those in ubiquitous computing environments.

## 2.4 Privacy in ubiquitous computing environments

A key attribute of ubiquitous systems, as identified by Langheinrich, is the co-mingling of ubiquity and invisibility: computing occurs everywhere, but should be seamlessly embedded into the environment [11, 12]. A possible solution to this is the development of "privacy-aware" systems, in which devices are able to identify the presence of smart devices that could be the source of privacy concerns, even if human users are unable to identify them [11, 12, 5]. Early conceptualizations of these systems require the establishment of a universally-accepted protocol for both the owners of ubiquitous computing devices, as well as the people whose privacy could be compromised by these devices. Similarly, Li et al. identify means through which smartphone users could minimize the amount of information that could be gathered by smart city devices through the use of cloud storage [14]. In conjunction with Langheinrich's proposed system, this provides a solid framework for privacy protection in ubiquitous computing environments, contingent on the widespread adoption of proposed protocols. In lieu of a universal protocol, the acceptance of which could prove quite challenging, Egelman et al. proposed an iconographic library by which sensors in ubiquitous computing environments might be able to indicate to individuals the type of data collection being done by a particular device [5], as a form of "active announcement" [12] (that is, the act of informing an individual when their privacy is potentially compromised). Eckhoff and Wagner provide another alternative to the aforementioned solutions, in which "privacy-enhancing technologies" or "PETs" are directly incorporated into the ubiquitous system [4]. Instead of relying on "active announcement," PETs instead minimize the potential for these devices to gather sensitive data about non-consenting individuals through data minimization, anonymization, encryption, and a wide range of other techniques. This can be understood to be a prototypical form of privacy by design in ubiquitous computing environments.

# 3. SURVEY

As previously mentioned, we have two research questions we hope to address in this paper. One is about the design space of "privacy by design" for urban sensors, and another is about the design space of "privacy display", i.e. how to convey data collection policy to people. We will use different approaches for the two research questions.

In our initial data collection, we used 3 factors (amount of data collected, accessibility of the data, and lifetime of the data) to describe certain data collection policies. To explore the influence of those three dimensions on people's attitudes toward a device, and measure if those three dimensions play a significant role in determining people's comfort level, we chose to conduct a survey. The survey consists of two parts: the first part hopes to study the influence of the three factors, and the second part studies the general expectation on data collection policy.

In the first part of the survey, we provided participants with several scenarios of privacy policies of urban sensors which only varied in the three previously listed dimensions. For each scenario, we picked one option from each dimension to generate a scenario. In total, we have 12 (2*2*3) different scenarios. We provided those scenarios to participants and asked them how comfortable they would feel walking around the camera based on a 5-Point Likert Scale.

In the second part of the survey, we wanted to reveal participants' expectation on privacy policy of urban sensors. Several open-end questions were asked, such as how long they thought was a proper life-cycle of the data and who they thought should have access to the data. The complete question list of this survey can be found in Appendix of this paper.

# 4. LAB STUDY

After validating the three factors we choose in the data collection policy, we want to study how different displays will infect people's understanding and attitudes towards the device. In our "privacy display" study, we believe that only providing participants with descriptions about privacy display is not intuitive enough and may not reveal participants' real attitudes towards the display. Therefore, we implemented a real hardware which was capable to collect information from the environment and convey the information via different displays. We did a lab study where such device with different displays was shown to participants and we interviewed to evaluate the efficiency of each display.

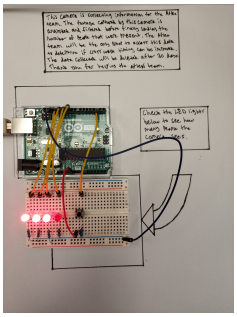
We narrowed our target device to study a street camera which detected the number of pedestrians in its view and dynamically controlled the traffic signal to improve the efficiency. In our imagined scenario for the device, it doesn't send any raw video footage to a remote facility, but only uploads number of people detected in its FOV periodly. Several types of privacy displays such as video, audio and LED display were implemented for the camera. Based on that, we implemented a 2-phase lab study in order to answer our research questions. In phase 1, the street camera with certain privacy communication approach was shown, and participants were asked to interact with the device for about 5 minutes. After that, the lab study would enter phase 2, where we interviewed the participants to evaluate their understandings of the data collection policy of the device.

## 4.1 Implementation

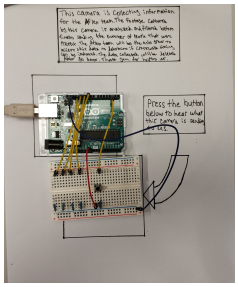
In the lab study, we implemented a real device in order to simulate the street camera. The device was built over a desktop computer. As we didn't have time and resource to produce a real street camera, we used a webcam instead. The devices used in this study consisted of a computer, a webcam, an LED display, and a speaker (shown in Figure 1). The computer with the webcam was used to both record the footage and process the images as well. An on-site algorithm [2] was used to detect human bodies in the footage and count how many people there were in the webcam's FOV. The computer then sent the results of the footage to one of the displays. In total, we tested five types of displays which is shown in Table ???. For all video displays, a monitor was used as the video feedback channel, and for LED and audio, we connected the computer with an Arduino microcontroller to control LEDs or get audio requests from buttons. When we tested a certain type of display, we disabled other display channels in our system to prevent any confounds.

In order to detect individuals from in the raw image and also blurring human faces, OpenPose, a human-pose-detection library from CVPR'17 [2], was used. We choose that library mainly because it provides very good false negative

Figure 1: Complete implementation of displays



(a) LED setting



(b) Audio setting

Figure 2: Non-video settings

performance. False negative performance is very important to our implementation, as if we failed to blur faces in the video in some conditions, participants would start questioning the device's privacy protection policy. The library is based on deep neural network and requires heavy computational power to provide real-time video processing. Thus, we took usage of a high-end graphic card inside our computer. Moreover, the software used to create the dynamic audio in our audio setting was gTTS. It is able to convert text string into an mp3 file with a more human-like voice.

### *negative*

In this display, we showed the raw video footage taken by the webcam to the participants. To communicate the privacy policy of the device, we put a rolling subtitle on the top of the video display saying "Your privacy has been taken into consideration." This was a vague argument which didn't convey any valid information and was considered as our negative setting, or control group. At the bottom of the screen, we showed the number of people the device had detected.

### *blur+negative text*

For this type of display, we used another layer in our algorithm to blur all sensitive information in the video feedback (i.e. human faces). All other settings stayed the same as the negative setting, which means that the rolling subtitle still didn't consist of any concrete information, and the number of people detected was shown at the bottom of the video feedback.

### *blur+informative text*

In this setting, comparing to setting "blur+negative text", we still blurred human faces, but we changed the rolling subtitle into a more informative one. In this setting's rolling subtitle, we described the data flow of the device in detail with information such as "what data is collected", "who will be accessing the data", "how long will the data be stored" and "how the data is being used".

### *LED*

In this setting, we didn't have any video feedback to the participants. Instead, we used four LEDs to show the number of people detected in the FOV (Figure 2a). If there were less than 4 people in the FOV, the number of lightened up LEDs would indicate the number of people detected, and if there were more than 4 people in the FOV, all LEDs would light up. As we disabled video feedback in this setting, we didn't have any rolling subtitles conveying information. To make it consistent with the video settings, we put the breadboard onto a piece of paper showing the same information as setting "blur+informative text".

### *audio*

For this type of display, we connected a button to the microcontroller and a speaker to the computer. Once the button was pressed, the speaker would say: "There are X people in the view" depending on the number of people detected. Similar to the LED setting, we also put the breadboard and microcontroller on a piece of paper to show useful information to the participants (Figure 2b).

## 4.2 Process

### *4.2.1 Phase 1 - Interact*

In this phase, we asked the participants to interact with the device we provided in the lab. As mentioned earlier in this paper, we had 5 versions of display. Each participant was assigned to only one of the displays. The participants was able to walk around the camera and watch (or listen to) the information conveyed by the display. To make sure that they could test the behavior of the device in different situations, all PIs were waiting outside the camera's view and would enter the view to test the camera if the participants felt necessary. To make sure that participants really believed the device was real and didn't try to say good words to please the PIs, they were told that the device was a prototype from a company named Aflex, and would be soon implemented in some neighborhoods in Chicago to dynamically control the traffic.

### *4.2.2 Phase 2 - Interview*

After participants finished interacting with the device, we performed a semi-structured interview to evaluate how much they understood the device's data collection policy as well as how much they believed it. During the interview, we asked the participants three sets of questions: one set that revealed their understandings about details in the dataflow, another set asking how they feel about this camera, and the last set that evaluated how much they believed the information conveyed by us.

For the first set, we focused on several aspects mentioned in our motivation section. The first aspect is sensitivity of

| # | Setting | Description |
|---|---|---|
| 1 | negative | Raw video footage + Your privacy has been taken into consideration." |
| 2 | blur+negative text | Video with faces blurred + "Your privacy has been taken into consideration." |
| 3 | blur+informative text | Video with faces blurred + informative rolling subtitle |
| 4 | LED | Number of lightened up LEDS = number of people |
| 5 | audio | Speak "there are X people in the view" once button pressed |

Table 1: Different settings of display in lab study

data moment. In this case, that dimension means what data was collected and uploaded by the "street camera" in our lab study. Below were the questions we asked:

- What do you think the camera is recording and what is it trying to analyze?
- What data do you think the device is sending to the Aflex team?

The second aspect is the accessibility of the data, which means "who can access the data being collected" in our case. We asked a single question for this dimension:

- Who do you think has access to the data?

The last aspect was about participants' overall understanding about the purpose of data collection and to verify if they had read the accompanying text if provided:

- Why do you believe this information is being collected?

We also wanted to evaluate how much participants felt comfortable about the camera given a certain display:

- Do you feel comfortable or uncomfortable walking near this camera?

Besides the effectiveness of conveying information, we also wished to evaluate how much a certain display was able to convince participants that the only the data that was claimed to be collected was actually collected by the device:

- Do you believe it is recording the number of people?
- Do you believe it is only sending the number of people?

## 4.3 Recruitment

Our recruitment occurred largely online, using various social media channels to reach out to potential participants. Given that both our studies were conducted on the University of Chicago campus in a space that required participants to have University of Chicago ID Cards, we chose to restrict our participant pool to current students and associated members of the university for whom this would not be an issue. We advertised our study on various large (100+ members) Facebook Groups for UChicago students, such as pages for particular class years and residential communities. However, since such advertising required participants to share their names and interact indirectly with a member of our research team (via their Facebook profiles), we recognized that this could create potential issues of biased responses or questions of confidentiality if this team member was directly involved in conducting the study. To avoid such issues, this team member was not present at the time of data collection, allowing us to be confident that the data gathered would be unaffected by prior interaction and completely anonymous to all members of the research team. This also resolved an issue presented by our compensation model, in which participants were compensated $5 for their participation in the 30-minute study, paid in cash or Venmo– since Venmo was also a not anonymous medium, the same member of the research team handled all payments to the study participants.

## 4.4 Ethics

The main ethical concern in our study is that a camera was recording participants in our lab. To prevent the leakage of footages containing participants' images, we apply two approaches. First, during the lab study, we didn't store any audio/video footage from the participants. As the camera was only processing the video on-the-fly, we didn't have any record of the video after the study finishes. Thus it is not possible that the actual footage will be disclosed. Second, we did not collect any identifiable information from the participants such as name, major, age, etc. Instead, we identified participants with codes, such as P1, P2, etc. Moreover, we revealed the real research goal after participants has finished the whole process, and participants had the right to drop the lab study at any time.

# 5. RESULT & DISCUSSION

In this section, we will present the results from both the interview and the survey and discuss about them. From the interview, we mainly want to understand how each displays affect participants' ability to understand the data collection policy of the device which includes the type, accessibility and lifetime of the data. Another dimension to be learnt from the interview is how participants trust the information conveyed under different types of displays. From the result of the survey, we analyze how three factors, data amount, accessibility and lifetime, impact participants' comfort level. Moreover, from the general questions in the survey, we reveal people's expectation of data collecting policy, i.e. their mental model of urban sensors.

## 5.1 Survey results

### *5.1.1 Influence of factors in privacy design*

In the survey, we provided several scenarios to the user which differed in 3 dimensions:

- What data is collected {raw footage; number of people}

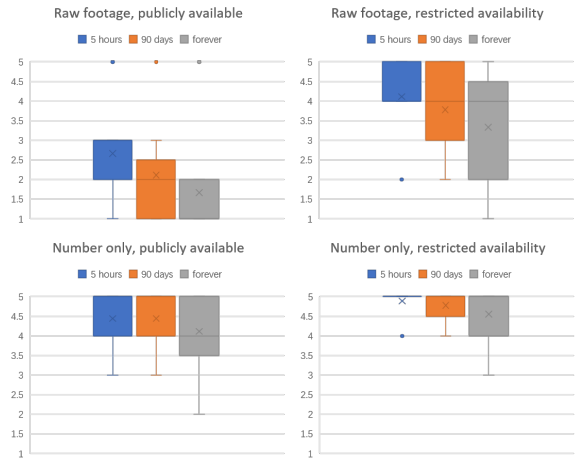



Figure 3: Box and whisker figure of comfort level result for each scenario

- Whether access to the data is restricted: {the data is publicly available; the data is only available to police/researchers}
- The length that the data is stored: {the data is stored for 5 hours; the data is stored for 90 days; the data is stored forever}

Those three factors are considered as independent variables in this study, and the Likert scale output (how much participants felt comfortable, 0-5) is considered as dependent variables. The result of this study is shown in Figure 3.

As we expected, discarding the raw footage, storing the data for shorter time and restrictions on data access have positive influence on participants' comfort level. To be more exact, from Figure 3, it is clear that participants feel much more comfortable after if the raw footage is discarded and only number of people is uploaded. As an example, when we constrain the other two factors to "publicly available, stored for 5 hours", the mean "comfort" grade by Likert scale raises from 2.6 to 4.5. Restrictions on data access has similar influence: the mean comfort grade by Likert scale increase by 1.5 if the data has limited access under the situation "raw footage, stored for 5 hours". We can also see from the graph that the longer data is stored, the less comfortable participants are. However, when we have other protective factors, especially only uploading number of people, the lifetime of data storage plays a relatively minor role on influencing participants' comfort.

To conduct a quantitative analysis on the data, an ordinal regression model to represent the influence of three independent variables on the comfort level by Likert scale was used. In order to achieve significance in all predictors, the researchers separated the lifetime dimension of the data into two sets: finite lifetime, 5 hours or 90 days, and infinite lifetime, forever. With this in mind, an ordinal regression model with 3 binary predictors and 1 response variable (5-option Likert scale) was created. The results are shown in Table 2.

From the values in Table 2, we can see that when using Bonferroni correction method at the 0.05 significance level,

| | p value |
|---|---|
| Video Recorded | 0.0000 |
| Accessibility | 0.0000 |
| Permanence | 0.0132 |
| Very Uncomfortable/Uncomfortable | 0.0000 |
| Uncomfortable/Neutral | 0.0000 |
| Neutral/Comfortable | 0.0000 |
| Comfortable/Very Comfortable | 0.0000 |

Table 2: Calculated p-values for each binary predictor

we can reject the null hypothesis. We can conclude that collecting raw footage, not restricting access on data, and holding data indefinitely will significantly impact an individual's comfortability with the device. This sanity check verifies that the predictors chosen will impact an individual's comfort level with a device.

From this regression, we can also produce the data shown in Table 3, which represents the probability of a policy falling into a Likert score. The top row describes the policy where raw footage is sent, the data is made publicly available, and the data is held onto indefinitely (the least privacy-protective situation). The bottom row is for the policy that data is analyzed on site before sending non-identifying information, the accessibility of the data is restricted, and the data is only stored for a finite amount of time (the most privacy-protective situation). From Table 3, we can see that there is a 79.65% chance that someone will be uncomfortable with the completely invasive policy and there is a 97.53% chance that someone is comfortable with the completely non-invasive policy.

This verifies that if that the policy is properly conveyed and the individual believes that this policy is actually being used, then we should expect every individual to be comfortable with the device. Conversely, if the privacy policy is improperly conveyed or there is no trust in the device, then the individual could develop a mental model of the privacy policy where they are likely to feel uncomfortable by the device. However, this model also shows that if the accessibility of data and the type of data can be conveyed to the individual and they can be convinced that the policy is actually in effect, then it becomes likely the individual will become comfortable near the device.

### *5.1.2 Participants' expectation of data collecting policy of urban sensors*

In the end of the survey, we also asked the participants several questions about their mental model of urban sensors' data collection. Several data options were given to the participants such as number of people, number of cars, number of vehicles, human faces, license plates and environmental information (humidity, temperature, etc.). The result of this question is shown in Figure 4. Among those options, we find that participants were most likely to accept number of cars, number of vehicles, and environmental information to be collected. This suggested that secondary features of video footage are not considered very privacy-invasive and are treated similarly as widely accepted features (weather, temperature). Two of the options, licence plates and human faces are found to be relatively privacy-invasive in our set-

| Video Recorded | Publicly Accessible | Indefinite Storage | Uncomfortable | Neutral | Comfortable | Group |
|---|---|---|---|---|---|---|
| TRUE | TRUE | TRUE | 0.7965 | 0.1196 | 0.0839 | Uncomfortable |
| TRUE | TRUE | FALSE | 0.5829 | 0.2130 | 0.2041 | Uncomfortable |
| TRUE | FALSE | TRUE | 0.3413 | 0.2498 | 0.4089 | Comfortable |
| TRUE | TRUE | FALSE | 0.1561 | 0.1843 | 0.6595 | Comfortable |
| FALSE | TRUE | TRUE | 0.1614 | 0.1880 | 0.6504 | Comfortable |
| FALSE | TRUE | FALSE | 0.0644 | 0.0967 | 0.8390 | Comfortable |
| FALSE | FALSE | TRUE | 0.0249 | 0.0416 | 0.9336 | Comfortable |
| FALSE | FALSE | FALSE | 0.0090 | 0.0158 | 0.9752 | Comfortable |

Table 3: Probability that each privacy policy would be assigned to a particular Comfort Level

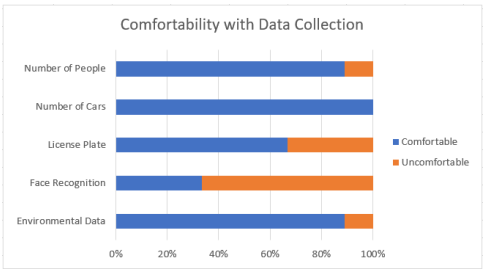



Figure 4: Distribution of Participants' comfortability with the collection of specific types of data

ting. Interestingly, we find that participants are more likely to accept licence plates to be recorded than human faces. We asked some open-ended questions after the survey, and it suggested participants already had a mental model that urban cameras were widely used by law enforcement institutions to track traffic rule violations and licence plates were already collected by many of them. We also asked several questions about the expected lifetime of stored data, or who should have access to the data. However, after the survey, we found that those were not valid questions, as we didn't give any context in those questions. Participants' mental models were quite different given different contexts. For example, one participant (p2) mentioned that for identifiable information, there should be a lifetime, but there was no reason to delete non-identifiable information in certain time span. Moreover, participants (p3, p6, p8) suggested that the lifetime should be different for publicly accessible data and data with restricted accessibility. There was another question about what information should be conveyed for those urban sensors. Besides all details about the data flow, one thing that was frequently mentioned by participants was transparency of the data. They would feel better if they knew where they could find the data collected by the camera, and the data available should be consistent for everybody in the city.

## 5.2 Interview results

### *5.2.1 Do participants realize what data is collected?*

Every participant was able to determine that the camera could detect the number of people present in its FOV. However, while each display type was successful at convincing users that it could detect the number of people, the different displays were believed to have different secondary purposes. The LED display had no secondary response– the two participants who assessed the LED display (P1 and P6) only mentioned sending the number of people present in the frame at some fixed interval. The audio display received two unique secondary responses: P3 claimed that it would send a snapshot of the footage whenever a change in the number of people occurred, whereas P8 assumed that it would send raw footage as well as audio along with the number of people present in the frame. The blurred display with informative text resulted in both participants, P4 and P9, claiming the device only sent the number of people and did not mention the device sending secondary information. The blurred display with negative text resulted in participants P2 and P7 claiming that the device sent raw footage to the Aflex team. Furthermore, P7 claimed that the device also sent audio to the Aflex team. P5, who was shown the unblurred display with negative text, claimed that it sent the foot traffic in any interval. P5 believed this was accomplished by sending raw footage to the Aflex team whenever the camera detected at least one individual. Overall, every participant was able to determine that the number of people were being collected by the camera. However, often times the participant would think that more privacy invasive information was being sent, even when information contradicting the assumption was provided.

### *5.2.2 Do participants know who will be able to access the data?*

The LED display and the negative text displays, both blurred and unblurred, were the only display types that resulted in a participant claiming that someone outside of the Aflex team or law enforcement would have access to the data being collected. P5, P6, and P7 thought that more people would access the data and claimed that some third parties would be either given the information or sold the information. Furthermore, none of the above participants actually read the accompanying text, indicating that they reached this conclusion using pre-existing knowledge or beliefs of the behaviors of cameras. P1 and P4 were the only participants to both have read the accompanying text and claim that the Aflex team and law enforcement were the only people to have access. P2, P3, P8, and P9 did not read the accompanying text, yet correctly claimed that the Aflex team and law enforcement would be the only groups with access to the data. This indicates that, similarly to P5, P6, and P7, these participants reached this conclusion using pre-existing knowledge and beliefs. It appears that participants are unlikely to read the accompanying text as only two of the nine participants did so. Overall, it seems that participants are unlikely to read the accompanying text and are likely to make judgment calls about a devices privacy policy with

varying accuracy.

#### 5.2.3 Do participants know how long will the data be stored?

Participants were not explicitly asked this question, but the information was provided in any non-negative text display. During the interview, two of the nine participants mentioned data storage length. The displays that resulted in this question, were the blurred display with positive text and the LED display. P4 actually mentioned how long the data would be stored and expressed minor relief in knowing that data would only be stored for a short period. The other participant P1 did not remember or know how long the data would be stored and asked the interviewer if they could provide the information. Upon being provided this information, P1 expressed a sense of interest, but did not ask any further questions. This seems to indicate that users will not seek out or do not think to seek out information about data storage length. This, in conjunction with the fact that we found it statistically significant on whether data is held indefinitely, seems to indicate that users may only feel strongly about this when it is overtly brought to their attention.

#### 5.2.4 How much do participants believe the information we conveyed?

There was a gap between what a participant thought the camera sent and whether or not they actually trusted that the camera would only send that. Every participant had been convinced that the camera actually determined the number of people in the frame and they all trusted that this information was sent. This indicates that it seems easy to convey that a type information is being collected and to convince people that this type of information is being sent. However, when the participants were asked if they believe that this is the only information being sent, only P4 agreed. While this was consistent with the participants who claimed that the camera sent secondary information, there were users who did not mention any secondary information being sent who claimed that they did not trust that this was the only information sent. Of the 4 participants who did not mention any other information being sent P1, P6, and P9 all mentioned a lack of trust that the number of people was the only information being collected. One explanation for this inconsistency maybe that the question itself provoked a sense distrust, making the participant feel that their original answer was incorrect.

#### 5.2.5 Comparison of different displays

##### Conveying the Privacy Policy

What type of data is sent: All five of the displays were equally capable at convincing users that the number of people was an important figure that the camera actually computed. Every participant, except for P3, thought the camera sent the number of people in the frame to the Aflex team. P3, who was given audio, thought that this information was used to determine when pertinent data should be collected. The only two display types that had every participant assigned to them correctly only claim that the number of people were being sent were the blurred display with informative text and the LED display. This indicates that these two displays are likely to be the most effective at conveying the policy of what information is being sent.

Who has access: From the discussion about who has access we can see that no display type appears to outperform the other. To accurately acquire this information the individual must read the accompanying text, but no display type showed consistency with getting a user to read this text. As a result, most users guessed using pre-existing knowledge to varying success.

How long: From the discussion about how long data will be stored we can see that it falls into a similar pitfall as accessibility. In order to obtain this information accurately a user must read the accompanying text. Not only were P1 and P4 the only participants to perform this task, but they were also the only participants to enquire or mention it.

With regards to conveying the privacy policy of a device, the blurred display with informative text and the LED display appear to be the most effective as they are the only displays to outperform the other displays in one of the above categories.

##### Developing Trust

Every device was able to acquire the trust required to convince users that the device was collecting a certain type of information. This was most likely accomplished by having the users interact with the device and seeing it correctly perform the task, instead of just having the users take the device at face value. Abstract policies, such as what information is not sent, which do not have a method of allowing users to validate that the policy is in effect left most participants unconvinced. The is most likely due to the fact that the current device has nothing to leverage and as a result requires that participants take it at face value. As a result, only P4 was convinced that the only information being sent was the number of people present.

No display seemed to be able to engender trust in the participants and as a result it appears that every display fails at developing trust.

##### Comfortability

Even though users had not been either fully informed of the privacy policy or did not trust that that was the privacy policy in effect, all but two participants, P6 and P7, were comfortable around the device. One common sentiment of the participants was that this technology was already quite pervasive and they had little control over it already. Another common sentiment was that they felt slightly weird about being recorded, but that it was not an uncomfortable sensation. P7 felt uncomfortable around the device that was blurred display with negative text. P7 felt that the device was very disconcerting and if they came across it in a wild setting would be very uncomfortable by the device. This is reasonable as this device does not convey any information or narrative about its purpose and is meant to raise a participants concerns about their privacy. P6 felt uncomfortable around the device due to an unforeseen issue: P6 felt that the device would not be easily noticeable and as a result would not be aware of its existence. This idea of being watched without be alerted to it made the participant very uncomfortable for a reason outside of the privacy policy we had fabricated.

From these results it can be seen that devices with a small display may cause people to feel uncomfortable due to being more inconspicuous. Furthermore, devices without any information or explanation may cause users to feel more uncertain about a device resulting in an increase in uncomfortability. Therefore, devices with large displays and informative text appear to outperform the converse with regards to comfortability

### *Overall Results*

From these results, it can be seen that overall, the blurred display with informative text is the most effective display. With regards to conveying a policy, the only other display that performed roughly as well was the LED display. However, the LED display had the side effect of becoming inconspicuous which increased discomfort around the device. No device significantly outperformed any other device at developing trust. As a result, the blurred display with informative text is the most effective display.

## 6. LIMITATION & FUTURE WORK

The main limitation for our study is that we only tested different display in a coarse-grained way. There are a large number of other detailed factors that will possibly influence people's comfort level and also the trust to the information we conveyed in our study.

The first main shortcoming is that we did not consider the modality of different displays. In our study, video displays used a monitor to show the information. Meanwhile, the LED and audio displays involved exposed hardware, such as LEDs and buttons on a breadboard, and all text was presented on a sheet of paper. Additionally, while all other displays constantly presented feedback, the audio display only provided feedback when a participant pressed a button. It is possible that different modalities may have affected people's comfort level and trust in unpredictable ways, which could be a confounding variable in our results.

The second main shortcoming of our study is that by focusing on elements of the design that would convey information, we disregarded design elements that would lead participants to trust the device. In our study, we did not explore the relationship between participants' trust and design elements of the display. Detailed appearance or visual design of the device could contribute to people's level of trust and understanding, which was not considered in our analysis, and could limit the generalizability of our findings across devices.

Given these limitations, there are various possible modifications that could be made to this study in future iterations. To address the issue of modality across displays, a future iteration of this study should use a singular mode in all cases, eliminating this confound; alternatively, a study could also be conducted to measure the effect of different modalities on a subject's level of comfort and trust.

As for the issue of visual design elements affecting a subject's trust of a device, a future study could be conducted to determine if varying these elements would change the outcome. For example, if the style or text of the rolling subtitle were changed, would this affect a user's inclination to believe it? Additionally, our fictitious company "A-Flex" does not necessarily garner any trust from participants, and may have even negatively affected their inclination to trust the camera. Would incorporating iconography associated with well-known, trusted brands (or perhaps untrusted brands) into the visual design of the device affect trust levels? Future researchers could attempt to address these questions using a modified version of our study.

Finally, it is worth noting that any future work on this topic should address the important distinction between the 'action' and 'perception' of a device: even when told what a device does (its 'action'), it is quite possible that a participant might not fully believe this, resulting in a differing conception of what the device does (its 'perception'). We found that this is particularly common in the case of cameras, especially in urban environments, as there is already a strong association of these devices with ideas of spying and privacy invasiveness. Future studies should take note of this, and explore not only how to communicate what a device does, but also how to minimize the difference between its action and its perception (that is, find how to get participants to actually believe the device does what it says it does).

Regarding the text display, we could revise the method of notification. We previously displayed the text as a running line centered above the video footage, but this could perhaps be difficult for users to read, as not all of the text is ever present on the screen at the same time. We could also make use of other modalities, such as LED's, to draw attention to the text. Perhaps we could replace the text entirely with some other way of conveying who collects the data and how it is collected, such as iconography.

For the usability study in particular, we could design more neutral questions. Perhaps the reason that participants were so skeptical of the privacy notification is that we asked the participants if they believed that the data collected specified by the privacy notification was the only data collected. This could perhaps be too pointed of a question, and we could revise the question to be "Do you trust or do not trust this privacy policy?" to minimize suggestibility. Another potential cause of skepticism was perhaps the camera itself, as cameras are known for capturing continuous footage, and this intuition may have defeated the privacy notification itself. We could vary the types of cameras used, or perhaps use different sensors entirely and gauge how trusting participants are of those sensors.

We could also increase the level of ecological validity in the future by avoiding a lab study, as lab studies may induce comfort towards the device. We could implement a camera and a privacy notification in a real urban setting, such as a traffic intersection, and gauge participant perception in that context, although it would be difficult to account for weather, time of day, and other extraneous factors that arise in a real setting. Hosub Lee and Alfred Kobsa, in their future work, suggested a mobile wearable device that tracked participant location and displayed various privacy scenarios depending on user location. To our knowledge, they have not done so yet, and could potentially be something we could adapt.

## 7. CONCLUSIONS

In this paper, we explore the design space of urban sensors in two aspects. The first aspect is how different data collect-

ing policies will influence people's level of comfort walking around them. We studied this research question with a survey that provided a number of scenarios that differ in data collecting policy and evaluated participants' level of comfort. We find that restriction on data access, discarding raw footage and finite data lifetime all have positive influence in people's comfort level walking around the camera. Switching from short lifetime to medium lifetime, however, doesn't have significant influence on the comfort level.

To study the effectiveness of different displays, we conducted a lab study with a real implementation of the camera with 4 types of displays, raw video, blurred video, LED and audio. Every displays except ones with "bad text" (non-informative about data collecting policy) has been sufficient in conveying the privacy collecting policy of the device. Among all of them, blurred video with informative rolling subtitle has been the most successful following by LED display and audio display. However, none of the displays have been able to make participants really believe in the privacy collecting policy conveyed by us. Participants tended to be suspicious on whether only the number of people was uploaded by the camera, which suggests that future work needs to be done to explore effective design to build people's trust.

# 8. ACKNOWLEDGMENTS

This project is a course project of the "Usable Security and Privacy" course in the University of Chicago. We would like to thank Prof. Blase Ur for introducing useful background for this projects and also usable security/privacy overall. He also provided valuable suggestions during this study. We also want to thank Mainack Mondal and Weijia He for allowing us to conduct our lab study in Young Memorial Building on Campus.

# 9. ADDITIONAL AUTHORS

# 10. REFERENCES

[1] O. Bates and A. Friday. Beyond data in the smart city: repurposing existing campus iot. *IEEE Pervasive Computing*, 16(2):54–60, 2017.

[2] Z. Cao, T. Simon, S.-E. Wei, and Y. Sheikh. Realtime multi-person 2d pose estimation using part affinity fields. In *CVPR*, volume 1, page 7, 2017.

[3] L. Da Xu, W. He, and S. Li. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[4] D. Eckhoff and I. Wagner. Privacy in the smart city–applications, technologies, challenges and solutions. *IEEE Communications Surveys & Tutorials*, 2017.

[5] S. Egelman, R. Kannavara, and R. Chow. Is this thing on?: Crowdsourcing privacy indicators for ubiquitous sensing platforms. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1669–1678. ACM, 2015.

[6] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo. Rethinking connection security indicators. In *SOUPS*, pages 1–14, 2016.

[7] A. Gaur, B. Scotney, G. Parr, and S. McClean. Smart city architecture and its applications based on iot. *Procedia computer science*, 52:1089–1094, 2015.

[8] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *12th Symposium on Usable Privacy and Security (SOUPS)*, pages 321–340, 2016.

[9] J. E. Gómez, F. R. Marcillo, F. L. Triana, V. T. Gallo, B. W. Oviedo, and V. L. Hernández. Iot for environmental variables in urban areas. *Procedia Computer Science*, 109:67–74, 2017.

[10] S. Gürses, C. Troncoso, and C. Diaz. Engineering privacy by design. 2011.

[11] M. Langheinrich. Privacy by designâĂŤprinciples of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[12] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing*, pages 237–245. Springer, 2002.

[13] H. Lee and A. Kobsa. Understanding user privacy in internet of things environments. In *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*, pages 407–412. IEEE, 2016.

[14] Y. Li, W. Dai, Z. Ming, and M. Qiu. Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, 65(5):1339–1350, 2016.

[15] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho. Urban planning and building smart cities based on the internet of things using big data analytics. *Computer Networks*, 101:63–80, 2016.

[16] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 1–17, 2015.

[17] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer networks*, 76:146–164, 2015.

[18] S. Spiekermann and L. F. Cranor. Engineering privacy. *IEEE Transactions on software engineering*, 35(1):67–82, 2009.