The Transparency Times: an Installation Promoting Transparency in Urban Sensing

Sasha Volkov
UC Berkeley
San Francisco, CA
sgvolkov@gmail.com

Andrea Gagliano
UC Berkeley
Seattle, WA
agagliano316@gmail.com

Smart city initiatives are underway worldwide, from Denver to Singapore to London to Oakland. Sensors, cameras, and microphones in the cityscape bring the promise of increased efficiency and improved security. These benefits also come with potential harms including privacy and security vulnerabilities, as well as the potential to exacerbate socioeconomic disparity. Communities should proactively engage in discussions around the development of smart cities to reap benefits from these technologies while minimizing harms.

We created an interactive installation to use as a participatory design probe to help inform the public about the potential concerns of smart cities. Providing a tactile and transparent way to engage with public use sensors resulted in users having deeper, more emotional and more thoughtful responses to potential privacy harms.

Smart cities, participatory design, critical design, IoT, sensors, privacy, connected cities

1. INTRODUCTION

Smart city initiatives are increasingly ubiquitous. Recent projects include monitoring pedestrian and traffic activities to create safer streets; detecting gunshots, car accidents, and flooding to better respond to safety incidents; measuring air quality to improve pollution; and, documenting homeless activities to better distribute human services. These initiatives build on the promises made by consumer Internet of Things (IoT) devices to increase efficiency, improve security, and provide lifestyle benefits. However, the public interaction of these projects brings concerns of individual privacy, cybersecurity vulnerabilities, reliability, and the potential to exacerbate widening socioeconomic disparity. This brings us to our primary research question: how can we use critical design to illuminate both the benefits and harms of smart city technology?

There are no easy solutions to these problems and no clear optimal trade-off between risks and benefits. The technologies underlying smart cities, including sensors, cameras, machine learning detection algorithms, and data infrastructure are ever-evolving and complex. The implications, especially secondary and tertiary implications, are not easily foreseen until they occur. In this paper, we will expose the benefits and potential harms of public use smart city technologies and provide a possible solution for increasing transparency and engaging the public in discussions around their development.

2. BENEFITS OF SMART CITY INITIATIVES

Public sensors and cameras are increasingly apparent in cities. Their usage portends the ‘enhancement of daily life.’ Some potential benefits include:

- Energy savings
- Increasing traffic and transportation efficiency
- Improving pedestrian safety
- Monitoring the environment
- Aiding police efforts
- Tracking usage of public infrastructure
- Improving physical security

When public sensors work properly, they have the ability to improve numerous services relied upon by millions of people. Moreover, they cut costs and free tax dollars to be spent on implementing new services.

3. CONCERNS FOR SMART CITY INITIATIVES

© Sasha *Volkov, Andrea Gagliano.*
Published by BCS Learning and Development Ltd. Proceedings of British HCI 2018. Belfast, UK

Through research with installation artists, privacy professionals, and academic papers, we developed a working list of some key areas of concern in smart cities to create a theoretical foundation to motivate our installation design.

3.1 Transparency of data being collected, how it is being used, and who is using it

Each city maintains its own set of rules and regulations around what data is collected, how it is shared, and what level of access the general public has. For example, the Array of Things project in Chicago has an online map that shows locations of live and planned sensors to promote transparency. Other questions remain: who has access to this data? What algorithms are used and for what purpose? These are more opaque.

Furthermore, not everyone monitored by public sensors has equitable access to these online resources. Without adequate disclosure it is impossible to expect an informed and consenting populace.

3.2 Tension between privacy and surveillance efforts to protect citizens and public spaces

There is a presumed expectation of anonymity in public spaces that has been thwarted by the introduction of sensing technologies. With the example of facial recognition software being used for capitalist gain and monitoring purposes, Greenfield argues that advancements in surveillance technology remove that promise (Greenfield, 2017). Such technologies are now capable of identifying one's gender, ethnicity, and even who they are. This level of continuous data collection is reminiscent of a modern-day *Panopticon*, a dyad wherein "one is totally seen, without ever seeing… [and where] one sees everything without ever being seen." (Foucault, 2008). Because these sensors exist in public spaces and are becoming increasingly pervasive, the only means of avoiding being sensed will be to avoid public spaces altogether.

There is an inherent paternalism in using a default option with no alternative. They are easier. While defaults remove the need to actively think about or make a choice, they also normalize that action. In doing so, they are ignoring the possible ethical or moralistic implications of that choice.

3.3 Unequal impact for people in different communities

Sensing technologies within city landscapes impact different communities in different ways. The homeless population, for example, spends more time on the streets than the average citizen, and may conduct different activities. Are they more susceptible to being tracked, and in what ways is that positive or negative? If smart city technologies are implemented in one neighbourhood over another, will one receive more attention, thereby distorting the balance of distributed public services?

The question of how public resources should be allocated remains largely at odds with the introduction of public sensors. Take the example of ShotSpotter, whose goal is to listen for gunshots and alert police of its location. Ninety communities across the United States have spent millions of dollars implementing it. However, arrests are rare, and access to data is limited. Moreover, police were unable to find any evidence of a gunshot between 30% - 70% of the time. With a cost of up to $90,000 per square mile per year, this begs the question of whether that money could be better spent elsewhere.

This issue extends to a multitude of technologies. For example, as of 2011, the city of Chicago had access to over 10,000 public and private surveillance cameras across the city. Studies have shown examples of abuse surrounding the inappropriate monitoring of citizens in their homes as well as the targeting of African Americans by camera operators. The cost of this program was $60 million.

3.4 Cybersecurity concerns of distributed IoT systems

IoT devices in public environments are highly susceptible to cybersecurity risks. IoT at the citywide scale consists of large networks of sensors. Such systems exist in physical (i.e. sensors) and digital (i.e. information architecture) realms, while also being accessible wirelessly through WiFi, Bluetooth, and/or radio communications. They pose increased risk for cybersecurity attacks over consumer IoT because of their criticality and their number of entry points. They run electrical power grids, traffic lights, and communicate with autonomous vehicles. If compromised, city inhabitants can experience serious physical harm.

Ghena, et al. (2014) intentionally attacked connected traffic lights connected to reveal their design flaws. They found that "an adversary can control traffic infrastructure to cause disruption, degrade safety, or gain an unfair advantage". This example highlights the complexity involved in creating and maintaining secure systems. City departments are not well trained in this line of work, nor do they have the money to compete with the high salaries of security engineers at leading technology companies. Furthermore, there is a tension between the longevity of city infrastructure such as roads, traffic lights, lamp posts, etc., which can last decades, compared with the fast paced, ever-evolving technology sector. Computer security in particular requires constant updates and security patches, counter to the pace of operations of maintenance for city infrastructure. Due to lacking regulation in the cybersecurity space, cities are left uncertain where and how to prioritize IoT security efforts.

Kim, et al. (2017) made the claim that the "the main challenges in security in the Internet of Things include heterogeneity, operation in an open environment, and scalability", which are all prominent attributes of city. Sensors are heterogeneous because of their diverse security requirements. Data transfer of a general temperature sensor, for example, is a much lower priority than the integrity and level of encryption required of data transfer from sensors monitoring and controlling an electric grid. They are also cheaper. Yet another contributor is that sensors that operate open environments mean adversaries have both physical and wireless access. Because multiple parties need access to that data, including city departments and law enforcement agencies, the result can be chaotic.

Kim, et al. developed a toolkit (Secure Swarm Toolkit) for building 'an authorization service infrastructure for the IoT' to help counteract some of these primary security concerns for large scale IoT. However, this toolkit can be 'downloaded and deployed by anyone with moderate knowledge of computer security,' meaning one needs to be moderately knowledgeable about computer security. This poses a security concern, given novices may not have the requisite knowledge to ensure security level protection.

The potential future of a novice community engaging with public use sensors is broad, like Gray Area's Data Canvas: Sense Your City project deploying a DIY sensor network. But, each sensor that is part of a larger system becomes an entry point to that system, thereby adding to the security threat. For example, we used a Raspberry Pi to build our installation. While it allows for innovative uses and user control, the Pi is highly susceptible to attacks. We directly experienced this when we SSH-ed into our Raspberry Pi one day and received the following message in our terminal:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
```

Figure 1: *Terminal warning message*

We are more experienced than novice programmers; yet, it remains unclear how to ensure security. There is a growing need for security at the city level and the novice level of such systems, particularly as DIY and open source sensor communities begin to emerge in opposition to government-driven smart city initiatives.

4. BUILD AND RESEARCH

4.1 Privacy Survey

We required a baseline of how the population perceives privacy in public spaces. We found a Pew study from 2015 that tackles attitudes and perceptions around online privacy, but it did not address sensors or cameras in urban landscapes. Our survey included Pew questions to benchmark against the existing data, and also included new questions focused on sensors in public environments. We surveyed 530 people over the age of 18 in the United States, weighting by gender. We found that respondents have become increasingly privacy-conscious yet are comfortable relinquishing that privacy for anti-crime and anti-terrorist efforts.

Respondents display more privacy-conscious behaviours today. In Pew's 2015 survey, 59% of respondents had ever cleared their browser cookies. This number increased to 83% in our survey in 2017.

However, only a small majority care about their privacy in public spaces. 61% of respondents consider it important to be able to go around in public without always being identified.

This speaks to when it is appropriate to give up one's' privacy. In this case, for security. More people approved of the use of sensors and surveillance cameras for anti-terrorist (81% approved of sensors/85% approved of cameras) and anti-crime activity (81%/ 82%) than for increasing efficiency (51%/ 52%) and improving the environment (54%/ 54%).

4.2 Low-Fidelity Prototype

A focus group of 12 comprised of academics, artists and journalists from across UC Berkeley was assembled to validate the goals of this project and hone our low fidelity prototype. This session introduced the harms and benefits of smart cities to the group and proceeded with a participatory design phase to think through ideas around how to repurpose newspaper boxes to be used for an interactive, educational prototype. The session was concluded with an informal think-aloud exercise, where participants were showed a cardboard prototype. The group was allowed to interact with the prototype, ask questions, and provide feedback based on their initial reactions and earlier ideas.

4.3 High-Fidelity Prototype

Incorporating our feedback, we acquired two newspaper boxes and outfitted them with a suite of sensors to create an interactive experience. A force sensor on the ground detected when someone was in front of the installation; sound intensity sensors measured ambient noise levels; proximity sensors determined when someone was approaching; two live streaming cameras watched people interact with the installation. Speakers inside were used to bellow messages at passers-by to grab their attention.

The newspaper boxes used screens in place of the newspaper viewing area to display real-time data from the sensors, in the context of near-future news stories. One box contained 'social good' data stories about monitoring the environment and helping the homeless. These were contrasted with the other box which showcased stories about surveillance and police monitoring. Our intention was to offer opposing narratives about how the same data can be used and for what purposes. We also included signage across the sidewalk notifying passers-by of data collection activities. The back of the sign had a terms of service (ToS) in print too small to read taken from the Chicago Array of Things Privacy Policy. This served as commentary on the lack the ability to opt-out, let alone the lack of consent offered by current smart city technologies. The ToS sign includes a signature line for a citizen to sign, yet is too far out of reach, furthering the commentary. These design choices were made to invoke reactions around consent and awareness.

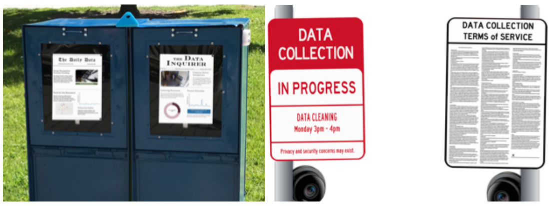

Figure 2: *Prototype in the field; data collection signage*

The prototype was piloted with several students for usability purposes, and then placed on UC Berkeley's campus - a public space - for three days. The goal of these observational days was to learn how people understood and reacted to the installation without any priming from the researchers. Many were curious about the repurposing of an otherwise ignored object; several showed concerns around their loss of privacy. Several comments were made around how "creepy" the installation felt. A few broader findings from our observations of over 40 passers-by include:

(a) Most participants noted never thinking about or noticing public use sensors or the data they collect. Many were unsure which stories were based on current sensor technologies.
(b) Physical interactions with the probe aroused a variety of emotional responses. They were most uncomfortable when seeing their own image. It left several with feelings of concern and paranoia.
(c) Sensors can be inaccurate and unreliable, even when higher quality. They are sensitive to climate and may collect data at different intervals from others performing the same tasks, thereby producing different results. This is a concern when policies are based on such data.
(d) Reliance upon WIFI is an issue for sensors and can cause quality and reliability issues.

5. CONCLUSION

The benefits of such smart city technologies are plentiful and far reaching. Yet, there are a number of potential harms society may be forced to grapple with, such as inconsistent or inexistent cybersecurity protocols, outdated technology, or privacy concerns regarding who has access to sensitive data. By providing a tactile and overtly transparent way to engage with public use sensors, we created a foundation for meaningful discussions which resulted in emotional responses to potential privacy harms, indicating that this is an area ripe for improvement from a citizen engagement perspective.

6. REFERENCES

ACLU, n.d., *What's wrong with Public Video Surveillance?,* https://www.aclu.org/other/whats-wrong-public-video-surveillance, (March 11, 2018)

Greenfield, A. (2017) *Radical Technologies: the Design of Everyday Life,* UC Berkeley, March 2017. Verso, Brooklyn, NYC, NY

Foucault, M. (2008). 'Panopticism' from Discipline & Punish: The Birth of the Prison. Race/Ethnicity: Multidisciplinary Global Contexts2(1). Indiana University Press (Retrieved March 12, 2018 from Project MUSE Database).

Whitney Museum of Art, Mitchell, M., Privacy: On the State of Surveillance, http://whitney.org/WhitneyStories/Cryptoparty, (April 28th, 2017)

Forbes, Drange, M. (2016), *We're Spending Millions On This High-Tech System Designed To Reduce Gun Violence. Is It Making A Difference?,* https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence/#1783b98131cb, (retrieved May 4, 2017)

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). *Green Lights Forever: Analyzing the Security of Traffic Infrastructure.* WOOT, 14, 7-7.

Kim, H., Kang, E., Lee, E. A., & Broman, D. (2017, April). *A toolkit for construction of authorization service infrastructure for the internet of things.* In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (pp. 147-158). ACM.

Kim, H., Kang, E., Lee, E. A., & Broman, D. (2017, April). *A toolkit for construction of authorization service infrastructure for the internet of things.* In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (pp. 147-158). ACM.

Pew Research Center, (2015), *Americans' Attitudes About Privacy, Security and Surveillance,* http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/, (retrieved March 20, 2017)

Digital Trends, Olewitz, C. (2016), *MIT's new sensor-loaded duct tape makes DIY electronics a snap,* https://www.digitaltrends.com/cool-tech/sensortape-sensor-packed-roll-of-electrical-circuitry, (retrieved May 5, 2017)

Illuminate.org, (2017), *Lightrail Project,* http://illuminate.org/projects/lightrail/, (retrieved May 4, 2017)