Can a City Invade Your Privacy?: Does the Rise of Smart Cities Mean the Fall of Privacy

Christopher A. Holecek
Wegman, Hessler & Vanderburg
6055 Rockside Woods Blvd., Suite 200
Cleveland, OH 44131

1. Introduction

In the 2002 film *Minority Report*, Tom Cruise starred as a police officer in the year 2054 in Washington, D.C. In the movie, a special police unit, known as PreCrime aimed to prevent murder by identifying and arresting potential murderers before an actual murder occurred. *Minority Report* (20th Century Fox 2002). Tom Cruise plays a police Captain overseeing the PreCrime unit which has reduced the murder rate in Washington, D.C. to zero by utilizing special humans who can "previsualize" crimes. In the film, a new prediction is generated which predicts that Tom Cruise's character will murder a man named Leo Crow in 35 hours. The rest of the movie consists of Tom Cruise attempting to resist arrest and prevent his fate from coming true in a futuristic smart city. The city in the film has implemented a citywide optical recognition system that both personally tailors advertisements and billboard to people who walk by, but also serves as a security measure for the government. In order to avoid this security measure, Tom Cruise eventually gets an eye-transplant. Although the film has been used by many a Criminal Law professor to challenge students to identify when a person has actually committed a crime, the film also grapples with other themes such as the role of preventative government in protecting its citizenry, the role of media where technology makes its presence boundless, and life in a city where privacy is nearly nonexistent.

While the technology and security measures seen in *Minority Report* seemed far-fetched in 2002, the same is not true today. For example, prior to the 2012 Olympics, London installed high-tech trash cans around the city. In addition to being bomb-proof and having LED advertising screens, the trash cans also had an analytics system embedded in them which could detect devices and observe their behavior, using a unique ID code called a MAC address that is embedded in every Wi-Fi enabled device, including smartphones. The system could track everything from the speed of the pedestrians, to the make of the phone they were using, to the frequency the person walked through the area. The systems allowed the contractor, Renew, to sell businesses data about the potential customers outside their doors, create personalized ads for people as they walked by, and also compile data about crowd movements. For example, if a Renew trash can knows that you frequent a certain restaurant, every time you walk by the trash can could show you ads for a similar restaurant nearby. Kelsey Campbell-Dollaghan, "Brave New Garbage: London's Trash Cans Track

You Using Your Smartphone". *Gizmodo*, Aug. 9, 2013. Once the public found out about Renew's ability to track their movements and habits, criticism eventually led to the elimination of the cans. But, the cities of New York, Singapore, and Dubai have similar programs. Ravender Sembhy, "Bin Company Renew Dumped for £4m Loss". *Express*, Oct. 13, 2013. Trash cans like Renew's are just the beginning of smart cities like the one in *Minority Report*.

A smart city is defined as a "city that engages its citizens and connects its infrastructure electronically." A smart city can integrate numerous technological solutions, in a secure way, to manage a city's assets, including but not limited to, "local departments' information systems, schools, libraries, transportation systems, hospitals, power plants, law enforcement, and other community services." In building a smart city, the goal is to use technology to improve the way services aid the public to improve the quality of life. Sam Musa, "Smart City Roadmap," Jan. 2016, available at https://www.academia.edu/21181336/Smart_City_Roadmap. In other words, smart cities utilize the "Internet of Things" on a large scale to make life easier for its residents. There are numerous cities around the world that are implementing smart city technology. In October 2017, the city of Toronto hired Alphabet Inc.'s urban innovation company Sidewalk Labs, to revitalize and redevelop 12 acres of industrial wasteland in Toronto's downtown. Sidewalk Labs' project includes autonomous vehicles that are summoned by residents, a thermal grid that does not use fossil fuels, and robotic delivery systems and waste management systems. Nichola Saminather, "Sidewalk Labs to start testing Toronto smart-city tech this summer, break ground in 2020." *Reuters*, April 9, 2018. Sidewalk Labs has described the project as the "world's first neighborhood built from the internet-up." Claudia Geib, "Alphabet Will Start Toronto Smart City Project This Summer. Residents Still Have Questions." *Futurism*, Apr. 10, 2018.

While smart cities, like the one in Toronto, have the potential to do a lot of good , they can also pose serious privacy concerns. Just as the Luddites in the 19th century could not slow or prevent the progress of technology by destroying weaving machinery, it is unlikely that anyone can prevent the implementation of smart city technology.

2. Benefits of Smart Cities

A lot of literature and media coverage of smart cities focuses on the potential privacy concerns and problems with smart cities. Smart cities, however, have the potential to drastically increase the quality of living for the vast majority of its residents. From decreasing traffic delays, to diagnosing and preventing potential epidemics before they start, to aiding the government in tracking down terrorists, smart city technology is almost too good to be true.

In 2012, London introduced the Split Cycle Offset Optimization Technique (SCOOT) System to its traffic signal network. The system, "allows individual traffic signals to detect vehicles passing along a road and combine with others to amend their signal timings on a second by second basis, in order to adjust traffic flows accordingly through an area, making journeys more reliable." In addition, SCOOT also introduced pedestrian countdown technology which detects large groups of people waiting to cross the street and changes traffic signal timings to allow them to move quickly. Through SCOOT, London has been able to drastically reduce traffic and pedestrian delays without compromising safety. "SCOOT System Helps London's Traffic Flow More Smoothly," *TrafficTechnologyToday.com*, Mar. 20, 2012.

Similarly, Israel, and several other countries, currently monitor the sewage that flows into its sewage treatment plants for diseases. In 2013, Israel found the polio virus in sewage samples from Rahat, a city in the Negev Desert close to the Egyptian border. Israel quickly opened an investigation searching for potential cases of paralytic polio as well as an unimmunized persons. "Poliovirus detected from Environmental Samples in Israel." *WHO*, June 3, 2013. In smart cities of the future it is entirely possible that the government can use sewage information to preemptively fight the spread of dangerous diseases and identify areas of specified drug usage.

Finally, with the advent and proliferation of smartphones, smart cities can fight crime in new ways. Although police have often asked the public for help identifying criminals, police in smart cities can engage the public even more effectively. For example, the two suspects in the Boston Marathon bombing were identified, in part, through the release of information and photos throughout the world. Shortly after the bombing, the FBI released photos of the two suspects, which were instantaneously shared thousands of times on Facebook and Twitter. Through the public's efforts, police eventually found the suspects—brothers Tamerlan and Dzhokhar Tsarnaev. Carolyn Presutti, "Multi, Social Media Play Huge Role in Solving Boston Bombing." *Voice of America*, Apr. 20, 2013. In future smart cities, law enforcement will likely be able to utilize the public to find criminals in more efficient ways.

These examples barely begin to scratch the surface of the what smart cities will be able to do. One thing is sure though, smart cities will change the layout and functionality of cities in numerous ways, many of which will be for the better.

3. Potential Privacy Concerns

While smart cities will improve day-to-day life in many ways, it will be done at a significant expense. For example, the three smart city technologies mentioned above also raise privacy issues. After all, traffic control systems such as SCOOT and sewage monitoring systems provide immense amounts of data to the government regarding the habits and movements of its people, while using the public to identify suspects can often go awry when the public misidentifies an innocent person as a suspect. These concerns cause one to wonder if smart cities may eliminate privacy as we know it.

Smart cities primarily use two types of information: aggregate data and individual/real-time data. In aggregate data collection, sensors aggregate data about specific places or things. Then the data is sent to computer networks which analyze large quantities of information to spot trends. Claudia Geib, "Smart Cities May be the Death of Privacy As We Know It," *Futurism*, Nov. 7, 2017. Systems such as SCOOT or sewage collection systems use aggregated data. As such, the data is effectively anonymous in that it cannot be used to track specific individuals or gain information about them.

However, smart cities will also utilize real-time data collection which focuses on individual data. Renew's trash can program, which was mentioned above, is an example of real-time data collection in that it identified and collected data of individuals to personally tailor ads for specific people. Cities are pursuing more initiatives to implement real-time data gathering programs. For example, Singapore has plans to require all cars to have GPS systems that will monitor the location of every vehicle at all times, plus speed and direction in order to allow the city to automatically charge cars for parking fees and tickets, as well as impose taxes on drivers based on how much they drive. Claudia Geib, "Smart Cities May be the Death of Privacy As We Know It," *Futurism*, Nov. 7, 2017.

The problems with both aggregate and real-time data collection is that people often do not know how much information they are giving away. Although the data collection practices of Facebook and other private companies are currently under scrutiny, when cities begin large scale data collection, who will be held accountable? Additionally, what happens when information collected by smart cities is lost or exposed by hackers through cyber-attacks? The data and information that cities will be collecting will be more personal and more sensitive than ever before, and it is certain that the information collected will eventually be stolen through cyber-attacks. After all, governments are not on the cutting edge when it comes to cyber-security, are they?.

Finally, what if governments begin using our smartphones to monitor what we say and do. Indeed, there is mounting evidence that smartphone companies and smartphone applications already are listening to your conversations, and personalizing your ads based on what they hear. See Sam Nichols, "Your Phone Is Listening and it's Not Paranoia." *Vice*, Jun. 4, 2018. So I ask, what do we do? Should we insist on any safeguards? If so, what types?

4. What Can We Do?

There is probably nothing that we can do to prevent or slow the implementation and development of smart cities and their attendant technological innovations. However, as lawyers we can still help our clients by ensuring that they know about the erosion of privacy and by encouraging them to be more careful regarding their own privacy. Similarly, we can advocate for laws which require government and businesses to clearly delineate the terms of their data collection.

But is demanding accountability a concern to most Americans? Research has shown that despite people's concerns about their privacy, most do little to protect it. Liesbet van Zoonen, "Privacy Concerns in Smart Cities," *Government Information Quarterly*, Vol. 33, Issue 3, July 2016. After all, the top five passwords of 2017 are (1) 123456, (2) Password, (3) 12345678, (4) qwerty, and (5) 12345. Kirsten Korosec, "The 25 Most Common Passwords of 2017 Include 'Star Wars'". *FORTUNE*, Dec. 19, 2017. Similarly, the most popular pin code is "1234" and most people use the same password for multiple accounts. Liesbet van Zoonen, "Privacy Concerns in Smart Cities," *Government Information Quarterly*, Vol. 33, Issue 3, July 2016. Additionally, people share their personal information on numerous media sites, despite their claims to not feel secure on Facebook..

As lawyers, we should insist that future smart cities implement more transparent and flexible data collection procedures. For example, the European Union (EU) recently enacted the General Data Protection Regulation (GDPR), which requires that all businesses in the EU share the type of data that they collect from residents and gain individuals' consent to use it. Similarly, GDPR gives EU citizens the right to be "forgotten." This means that EU citizens can have all of their personal information removed from any database if they so choose. It is imperative that we demand cities and businesses implement laws like GDPR to ensure that they are clear on what they are doing.

5. Conclusion

Smart cities are the cities of the future. They are inevitable, and the tangible benefits are apparent. But can we create smart cities without undermining the protections afforded to us under our federal and state constitutions? Answering that question will be an ongoing challenge to our profession for decades to come.