Smart City or Surveillance City: Holding Smart Cities Accountable When it Comes to Privacy

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Lily Malinowski

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

STS Research Paper

Introduction

As cities begin to grow beyond their capacities, it is essential to form ideas about how to utilize technology to mitigate societal problems such as overcrowding and global warming. Engineers and researchers have coined the term “smart city” to describe a solution which addresses three aspects: sustainability, smartness (context aware economy), and inclusiveness (Arroub et al., 2016). Bringing this concept to life would consist of automating many processes and implementing technologies like sensors which would allow governments to better monitor problems such as weather and crime to identify potential problems before they arise. While this predictive and preventative strategy is quite convenient and innovative, it is important to consider the downside – violation of citizen privacy.

When considering privacy in today’s world, a smartphone is now a daily tool used for communication, and the amount of personal data transmitted through each device ranges from financial information to home address to past purchase history. While data can be used to make peoples’ lives more convenient, it is imperative to know what companies do with such data to keep users' information secure. If data privacy is already a concern today, it is important to investigate what laws are being made to hold companies accountable before technology begins to be implemented in every aspect of society.

Methods

Questions posed in this research paper consist of: How does implementation of smart cities and their automated sensing technologies violate human privacy? How are American citizens responding to that violation of privacy and can the wicked problem of privacy ever be tamed? To further explore how the implementation of technology may violate human rights, a literature review of past scholars weighing how privacy fits into the wicked problem framework

is used. Keywords of "privacy," "smart city," "privacy as a wicked problem," and "American opinion on human privacy" is utilized to find published journals. Some journals are used with expertise in smart cities, smart sensing capabilities, and American opinion while others discuss the wicked problem framework both alone and past work relating privacy to the wicked problem framework. To fully explore the problem, the idea of smart cities is discussed followed by the definition of a wicked problem and how privacy fits into that definition. After exploring privacy as a wicked problem, American opinion around human privacy is discussed and finally concludes with why wicked problems eventually must be solved and methods past scholars have proposed to strategize how to do that.

Background

Currently in the United States, privacy law is significantly underdeveloped but is constantly growing and evolving. As of now, the development of privacy law is largely dependent on a dialogue between the courts and legislature – where courts will occasionally define new interpretations of privacy rights (Solove & Schwartz, 2011). The development of technology also plays a big role in determining what privacy laws will be necessary in the future as well as other countries' laws being a potential model for how the current United States law can be improved.

Regarding federal law, notable laws currently enforced consist of the Electronic Communications Privacy Act of 1986 which prohibits the unauthorized interception of communications with limited talk about electronics (Rep. Kastenmeier, 1986) and the Gramm-Leach-Bliley Act of 1999 which requires privacy notices when financial institutions give user data to other companies (Sen. Gramm, 1999). There also exists the Children's Online Privacy Protection Act of 1998 which restricts websites gathering information from children under 13, but it contains no mention of privacy as it relates to adults. The consensus is that privacy law is

significantly limited in the US and is found mostly in state laws, if at all. International law utilizes two main approaches to privacy law: omnibus (comprehensive approach to privacy which spans all industries and contexts) and sectoral (regulates information based on industry and context) (Solove & Schwartz, 2011).

While it is essential to look at the laws currently in place, it is also important to note the public opinion on privacy. According to a survey by the Pew Research Center, 81% of U.S. adults feel they have little to no control over data that companies collect about them (Atske, 2019). Based on the survey, it is apparent that there are significant concerns in just owning just a cellular device/computer. If technological innovation is advancing beyond the privacy policies and laws that are holding companies accountable (Privacy & Technology, 2022), then all human privacy may be in jeopardy.

Wicked Problem and Privacy

In 1973, scholars Rittel and Webber coined the term "wicked problem" to describe the complex process of attempting to diagnose a problem which spans all aspects of society. In the paper, they defined 10 characteristics of a wicked problem, including: that there exists no definitive problem formulation, solutions to the problem aren't definitively "true" or "false," and that the problem is notably unique (Rittel & Webber, 1973).

The most seen paper is usually formatted by first defining the problem (whether that be sustainability, poverty, or privacy). Then a paper will outline and introduce Rittel and Webber's 10 characteristics and then outline in bullet points how the defined problem either meets or doesn't meet the criteria. Then is usually where the papers diverge – some use the framework to simply describe the problem in a measurable way, explore the concept of the problem, or provoke debate and incite social change (Lönngren & van Poeck, 2021). Other discourse around

wicked problems includes theories of how to solve them such as an article written by Conklin which offers steps on what he phrases how to "tame" a wicked problem. These papers usually again outline Rittel and Webber's problem outline, but then offer an approach to make the problem seem less complex.

There are also many critiques of wicked problem framing such as Turnbull and Hoppe's paper arguing that the term "wicked" may be stretching the concept too far and defining how policy workers define and solve complex societal problems. While wicked problems may be complex and overwhelming due to their intertwinement with all aspects of society, policy makers must define some kind of way to solve them – that a weak solution is better than no solution (Turnbull & Hoppe, 2018).

Results and Discussion

Smart cities in their proposed form make bold promises to enhance all aspects of society and yet they have significant downsides which aren't as significantly spoken about- one of them being the clear violation of human privacy. While Americans have varying opinions regarding privacy, the problem of privacy is potentially *tamable* but never *solvable*. In order to solve it, citizens must hold large companies and governments accountable when it comes to privacy through speaking out, voting, and policy making because it is apparent that governments and companies won't make the moral decisions necessary to protect human privacy themselves.

What is a smart city?

A smart city, one which works to implement automated sensors and monitoring devices to allow "smart sensing" and predictive capabilities, is being discussed globally as a way to implement modern technologies into everyday life. As IBM defines it, a "'smart city' is … the use of information and communication technology to sense, analyze and integrate the key

information of core systems in running cities [and] making an intelligent response to different kinds of needs … daily livelihood, environmental protection, public safety" (Su et al., 2011).

Concrete steps are being taken to actualize the concept of a smart city – the "Internet of Things" is a "cyber-physical mega-infrastructure … interconnecting physical and virtual things *including* humans" (Carr & Lesniewska, 2020). Essentially the physical objects may consist of sensors, cameras, monitoring devices, humans, and the virtual things are the way the devices communicate whether that be with each other, the cloud, or a data reserve system. While smart cities are not being fully implemented yet, the Internet of Things (IoT) is being tested through applications; for example low power wide area networks (LoRaWAN) allow for lower power, low cost, and low complexity devices that can communicate over long distances (Haxhibeqiri et al., 2018). The concept of a smart city seems like it exists in a distant future, but rather the technology used to actualize it is advancing much faster than expected.

A smart city seems to promise a lot of benefits- streamlining the process of urban planning. First, a smart city essentially promises to elevate each aspect of a city by improving technology in transportation, housing, medical treatment, clean energy/waste management, and much more. Utilizing the IoT sensor network, traffic management can be streamlined automatically changing traffic lights based on the current flow of traffic to mitigate vehicle fuel usage and reduce wait times (Su et al., 2011). Sensors used in a medical setting could count inventory, manage data collection, and strengthen the healthcare system (Su et al., 2011). Creating a wireless city – one that has WiFi throughout – would allow for citizens and tourists to utilize that WiFi along with allowing constant video surveillance with the goal of mitigating crime and increasing emergency response times. These are just a few of the benefits of

implementing a smart city – seamlessly integrating technology in everyday life in order to address common societal problems like sustainability, transportation, and medical problems.

A smart city in theory sounds like a promising idea – using technology to address all problems that currently exist in a city. Because there are so many benefits, it is important to consider potential downsides of implementing a smart city. First, there are the endless amounts of technical questions that come along with utilizing technology. Will technology make all the decisions? How involved will the government be in decision making, will they lead the technological implementation or will they still have a more involved role like they do today? How can one even begin to answer these questions given the fact that it is a completely novel idea? While smart cities are backed in some technical research, it appears that there are simply too many unanswered questions to safely begin to implement one. Continuing on the technical aspect, the other pressing issue is the ethical issues associated with a smart city. Informed consent from citizens is absolutely necessary when implementing a tool that completely affects their livelihood. Installing technologies that collect lots of privacy-sensitive information and also control city facilities and their lives is a powerful, but also dangerous tool (Zhang et al., 2017). Constant surveillance and monitoring would disclose very personal information about citizens' lifestyles. There are many potential consequences to consider when discussing a smart city, and weighing both the positives and negatives can ensure a more balanced solution.

While installing smart sensing and vast networks of computers which can communicate faster than human managed data might seem like a catch all solution, it may lead to more consequences than engineers and scholars are able to predict. Not to mention, research indicates that the only way to transform urban processes is by having better urban governance. Perhaps instead of using new technology to fix a problem, it would be better to organize stronger

collaboration between governments and their stakeholders (Anthopoulos, 2015). When thinking about a problem it is important to not only consider the practicality and execution of the solution, but also the potential ripple effects that may be produced by implementing said solution. It is important to consider if using technology to solve societal problems is even feasible to begin with.

What is a Wicked Problem?

In 1973, scholars Rittel and Webber coined the term "wicked problem" which consists of societal problems- including all public policy issues that can never be solved but rather are "re-solved over and over again" (Rittel & Webber, 1973). Wicked problems are defined based on ten main characteristics all cited from Rittel & Webber:

1. There is no definitive formulation of a wicked problem
2. Wicked problems have no stopping rule
3. Solutions to wicked problems are not true-or-false, but good-or-bad
4. There is no immediate and no ultimate test of a solution to a wicked problem
5. Every solution to a wicked problem is a 'one-shot operation'; because there is no opportunity to learn by trial-and-error, every attempt counts significantly
6. Wicked problems don't have an enumerable (or exhaustively describable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan
7. Every wicked problem is essentially unique
8. Every wicked problem can be considered to be a symptom of another problem

9. The existence of a discrepancy representing a wicked problem can be explained innumerous ways. The choice of explanation determines the nature of the problem's resolution
10. The planner has no right to be wrong

Based on these ten characteristics, numerous scholars have used Rittel & Webber's framework to define common societal problems such as education, global warming, poverty, etc. as wicked problems.

Privacy as a Wicked Problem

First in order to define privacy as a wicked problem, it is important to define what privacy is. "'Privacy is often thought of as a moral right or a legal right' … one's ability to control information about oneself" (Bélanger & Crossler, 2011). Privacy as a definition is quite subjective and spans numerous aspects of life. There are also different categorizations of privacy: privacy of a person, personal communication privacy, personal data privacy. Additionally there are other methods of maintaining that privacy such as "anonymity, fair use, controlled access, and use for integration" (Bargh et al., 2015) which companies can define and use to maintain trust with their users, but they can also utilize these to find loopholes to violate human privacy. Potential consequences of violating human privacy are identity theft, stealing financial information, and exposing personal communications (Acquisti et al., 2015). In an in person communication, users can trust that they are only talking to the people in the room. In the case of online communications, it is safe to assume that all data is being tracked and no conversations are absolutely private.

Privacy in a Judicial Setting

"Governance of digital technologies has emerged as one of the 'wicked problems' of our time" (Carr & Lesniewska, 2020). As technology advances rapidly, it is essential to be constantly considering how to uphold high standards to protect human privacy. In a study about information sharing in a judicial setting, scholars aim to demonstrate how transparency through information sharing can garner public trust in the context of government or scientific organizations. "Transparency … is now essential to many functions of democracy: participation, trust in government, prevention of corruption, informed decision making…" (Bargh et al., 2015). So a foundation of democracy is sharing of information to citizens to foster trust within their governments, that people have a say in how the government is run. While it is important to be transparent about certain information, there are also "information systems that process, e.g., collect, enhance, store, and share, privacy sensitive information (like names, email and postal addresses, dates of birth, geo-locations, bank account numbers, photos and political/personal opinions)" (Bargh et al., 2015) which could be potentially leaked or breached. The study continues to define how information sharing and lack of privacy fits Rittel and Webber's ten criteria. For example for point (3) of the wicked problem framework, they point out that the solutions implemented in the Data Protection Act 1998 and EU Data Protection Directive 95/46 does not clearly define what is "personal" data (Bargh et al., 2015). While sharing information can be useful and powerful, it also can be dangerous and violate the trust between the government and citizens. In an ideal world, the study concludes that there should be a "non-zero-sum relation between transparency and privacy… that successful privacy protection solutions do not necessarily prevent/obstruct data dissemination" (Bargh et al., 2015). While in a perfect world this solution would exist, it simply does not, which makes the issue of privacy in the context of a judicial system a wicked problem.

User Interactions with Privacy in America

In terms of American privacy laws, the ones that exist do not explicitly cover all rules and scenarios. Even the US Constitution does not "mention the word *privacy* but rather security against instructions in the fourth amendment (search and seizure)" (Alaqra, 2018). But the question is: how do Americans feel about the current state of privacy laws or their privacy more generally?

After the September 11, 2001 terrorist attack, the Patriot Act was created to allow the US government to detect and prevent terrorism. Because of the severity of this event, executive agencies have focused more heavily on finding ways to mitigate terrorism while also protecting personal privacy. In the days after September 11, 78 percent of Americans believed that investigating terrorist threats is more important than their personal privacy (Best et al., 2006). However, others expressed significant concerns about the violation of their civil liberties. However, over the span of the next 4 years following September 11, the percentage of Americans willing to take "whatever steps necessary [to prevent terrorism and have their privacy invaded]" significantly declined 31 percent. Based on this statistic, it seems as though concerns with privacy are a fluctuating scale- that the event and situation heavily dictates how sympathetic Americans are to having their rights violated for the benefit of the country. As time further separates them from a traumatic event though, their concern for personal rights returns to a baseline level of concern. The least popular type of government surveillance is that of monitoring personal communications. Personal communications include emails, virtual chat rooms, phone calls, and text messages.

One of the largest issues given privacy is that there exists what is termed "privacy uncertainty"- due to advances in technology the data collection and usage of personal

information is completely invisible (Acquisti et al., 2015). If people have no knowledge of their information being tracked, then they are likely uncertain of how much information they are sharing. The second pressing issue is the contrasting desire of people as social animals to share information as a way to connect with one another (Acquisti et al., 2015). Due to the rise of social media, Americans want to share their lives on social media apps like Instagram, Snapchat, and TikTok.

One study was conducted that proved individuals are more likely to reveal personal information on a website with a more rudimentary design than a professional interface, even though participants deemed the formal website to seem safer (Acquisti et al., 2015).

Privacy is heavily dependent on the environment that the user is in. If a recent event has significantly violated a user's privacy, then citizens are more likely to be weary of privacy violations. However, because information collection is almost invisible, people may not even be aware of their personal boundaries being compromised.

Taming a Wicked Problem

In the context of smart cities and urban planning, cities appear to be the "level at which solutions to wicked problems need to be produced" (Anthopoulos, 2015). Governments are given the role of solving complex societal (and therefore wicked) problems. While these wicked problems are intertwined heavily with societal problems, action must still be taken to attempt to mitigate their disastrous effects. "Rather than 'solve' them, we work instead to 'tame' them by dealing with a discreet aspect of the larger problem, or to 'cope' with them by utilizing existing institutions and mechanisms" (Carr & Lesniewska, 2020). There have been numerous scholars who have worked to develop taming strategies which will be further discussed in this section. All societal problems have to be solved eventually by policy analysts, and all of those problems are

considered wicked (Catron, 1981). Catron's paper further pokes holes in Rittel and Webber's initial problem formulation, first pointing out that planners and analysts are constrained by many variables: money, resources, time, expertise, political sensitivity, and more. While it is easy to justify why a problem is wicked, there are still people tasked with solving each problem with limited resources, therefore strategies must be created to address and mitigate these problems even if it is not plausible to completely eliminate them.

In the study discussed above about privacy and transparency with data in the judicial system, the Bargh carried out a legal study which settled on allowing privacy laws to scientists using the data for research because they are "less susceptible to data misuse, misinterpretation, and privacy breaches" (Bargh et al., 2015). By strictly imposing clear restrictions on where data can and cannot be shared with, the problem of privacy can begin to be tamed. In the study, they also developed a tool to perform checks to minimize the amount of privacy violations in the data distribution process. In this way, they actually used technology to keep technology accountable. Bargh concludes the paper "[the] search for a mix between transparency and privacy … was not focused on finding the correct balance point but was aimed at finding a realistic point" (Bargh et al., 2015). In essence his statement captures the meaning of taming a wicked problem. While there may be millions of solutions, all imperfect, it is important to simply pick the most practical and realistic method to tame a very wicked problem.

Limitations and Future Work

Despite reaching the idea that privacy while deemed wicked by some must be solved, the context of the research discussed solely speak to an American demographic. American citizens are living in a democratic government where it is very much encouraged to vote and speak up about government officials, laws, and their rights. With free speech, the ability to voice citizen

opinion (within reason), is unpunishable which is not a privilege lucky enough to be granted in all other countries. For example, during December 2022 in China protesters were monitored and identified using cellular devices and surveillance cameras. The protesters were named and confronted, now frightened to speak up or attend future protests. In countries like China, where free speech is talked about, but often governments imprison people for speaking out against the government a solution as this may not be so feasible. To expand on this research in the future, it would be essential to look at privacy laws and opinions of citizens in different countries as the implementation of smart cities is not just in the

Conclusion

Smart cities, while just a concept right now, are slowly beginning to be implemented through various technologies such as the Internet of Things (IoT) utilizing sensors with smart sensing capabilities. While the implementation of this concept promises a lot of benefits, its potential consequences are important to consider, especially the violation of human privacy. Privacy has been defined as wicked by multiple scholars and although it is deemed unsolvable, policy makers still must work to produce potential solutions by using problem taming methods. Ultimately, the problem of privacy is never completely solvable but through strict and clear government regulations on privacy policies and citizens speaking up when they feel their civil liberties are violated can hold companies accountable for preserving human privacy.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Alaqra, A. S. (2018). *The Wicked Problem of Privacy: Design Challenge for Crypto-based Solutions*. http://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-67134

Anthopoulos, L. G. (2015). Understanding the Smart City Domain: A Literature Review. In M. P. Rodríguez-Bolívar (Ed.), *Transforming City Governments for Successful Smart Cities* (pp. 9–21). Springer International Publishing. https://doi.org/10.1007/978-3-319-03167-5_2

Bargh, M. S., Choenni, S., & Meijer, R. (2015). Privacy and information sharing in a judicial setting: A wicked problem. *Proceedings of the 16th Annual International Conference on Digital Government Research*, 97–106. https://doi.org/10.1145/2757401.2757425

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/10.2307/41409971

Best, S. J., Krueger, B. S., & Ladewig, J. (2006). Privacy in the Information Age. *Public Opinion Quarterly*, *70*(3), 375–401. https://doi.org/10.1093/poq/nfl018

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: Learning from climate change governance. *International Relations*, *34*(3), 391–412. https://doi.org/10.1177/0047117820948247

Catron, B. L. (1981). On Taming Wicked Problems. *Dialogue*, *3*(3), 13–16.

Haxhibeqiri, J., De Poorter, E., Moerman, I., & Hoebeke, J. (2018). A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors (Basel, Switzerland)*, *18*(11), 3995. https://doi.org/10.3390/s18113995

Lewis, S. (2008). The Tissue Issue: A Wicked Problem. *Jurimetrics*, *48*(2), 193–215.

Lönngren, J., & van Poeck, K. (2021). Wicked problems: A mapping review of the literature. *International Journal of Sustainable Development & World Ecology*, *28*(6), 481–502. https://doi.org/10.1080/13504509.2020.1859415

Rep. Kastenmeier, R. W. [D-W.-2. (1986, October 21). *H.R.4952 - 99th Congress (1985-1986): Electronic Communications Privacy Act of 1986* (10/21/1986) [Legislation]. http://www.congress.gov/

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, *4*(2), 155–169.

Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., & Seskar, I. (n.d.). *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study*.

Seager, T., Selinger, E., & Wiek, A. (2012). Sustainable Engineering Science for Resolving Wicked Problems. *Journal of Agricultural and Environmental Ethics*, *25*(4), 467–484. https://doi.org/10.1007/s10806-011-9342-2

Sen. Gramm, P. [R-T. (1999, December 11). *S.900 - 106th Congress (1999-2000): Gramm-Leach-Bliley Act* (11/12/1999) [Legislation]. http://www.congress.gov/

Solove, D. J., & Schwartz, P. M. (2011). *Privacy law fundamentals*. International Association of Privacy Professionals.

Su, K., Li, J., & Fu, H. (2011). Smart city and the applications. *2011 International Conference on Electronics, Communications and Control (ICECC)*, 1028–1031. https://doi.org/10.1109/ICECC.2011.6066743

The State of Consumer Data Privacy Laws in the US (And Why It Matters). (2021, September 6). *Wirecutter: Reviews for the Real World*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Turnbull, N., & Hoppe, R. (2018). wicked problems—Turnbull and Hoppe, 2018. *Policy and Society*. https://doi.org/10.1080/14494035.2018.1488796

Walls, H. L. (2018). Wicked problems and a 'wicked' solution. *Globalization and Health*, *14*(1), 34. https://doi.org/10.1186/s12992-018-0353-x

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM