NEW AMERICA

April 2019

Smart is Not Enough

How to ensure the technologies of the future don’t break our cities (and us with them)

Natasha Cohen & Brian Nussbaum

Last edited on April 04, 2019 at 9:34 a.m. EDT

Acknowledgments

The authors would like to thank Robert Morgus and Ian Wallace for their assistance with the formation and development of this project. We would also like to thank all the experts we interviewed for this project and the reviewers who provided us with feedback.

This paper is part of New America's Cybersecurity Initiative. The work of the Initiative is made possible by support from the Microsoft Corporation, JPMorgan Chase and the William and Flora Hewlett Foundation, and the through our partnership with Florida International University.

About the Author(s)

Natasha Cohen was a fellow in New America's Cybersecurity Initiative, where she focuses on State, Local, Tribal, and Territorial (SLTT) cybersecurity policy issues. She has published on best practices in SLTT cybersecurity governance, national and state compliance and regulation, and economic development. Her clients included government agencies, Fortune 100 companies, and small to midsize rms operating in the United States and international spheres.

Brian Nussbaum is a fellow in New America's Cybersecurity Initiative. He is also an assistant professor in the College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC) at the University at Albany, an affiliate scholar with Stanford's Center for Internet and Society (CIS), and a former intelligence analyst.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

Contents

Introduction

Imagine a city where subway cars connected to each other, synchronizing transfers based on average transport time between arrival of one train and the departure of another; where streetlights varied in brightness based on ambient light and population presence, saving the city millions of dollars and decreasing energy requirements; where your phone could direct you to the nearest parking spot to your next meeting.

For years, smart city vendors, engineers of many stripes, and thought-leading urbanists have been telling us a wonderful story about the smart cities to come. These stories are filled with efficiencies and savings, targeted and personalized services, frictionless interactions and payments, and infrastructure that learns and adapts to changing usage and needs. We are not there yet—important technologies required for this vision at scale remain just over the horizon. And some of the challenges are as much political and cultural as technical—how to deliver last mile fiber effectively in many places,[1] for example, is still an open question, as is the challenge of automating or computerizing aging and poorly maintained infrastructure.[2]

But the smart city is no longer purely science fiction either, and building ever smarter cities is a major priority globally. More than 26 smart cities are expected to be established by 2025; Singapore wants to become the world's first "Smart Nation."[3] Yet, the technology needed to build smarter cities and nations carries major risks. As security expert Bruce Schneier has observed, when "smart" can translate loosely to "hackable," this future takes on some new connotations.[4]

But the smart city is no longer purely science fiction either, and building ever smarter cities is a major priority globally.

Despite increasing concern from the information security community, it is far from clear that even the smartest of U.S. cities are in a position to deal with the full range of new risks that the technology may bring. The required financial, social, security, operational, legal, and policy innovations needed for smart cities to deliver on their aforementioned promises do not appear to be moving at the pace of innovation of the technology.[5] It is important that city managers,

activists, engineers, and policymakers recognize that many of the most important hurdles to achieving the promise of the smart city will not be technological problems.

This paper will look at smart cities with a critical eye, examining this promise of a smart city and asking the questions we will have to wrestle with as technology becomes more and more integrated into our daily life in cities, states, and countries. We will also highlight some of the areas that need further attention if we are to continue the rapid deployment of smart city technology in our cities, states, and countries. We hope that this paper informs the range of stakeholders in smart cities—from the engineers who build the technology, to the city leaders who are responsible for making the best decisions for their constituents, to the activists and policymakers who look at the various aspects of what a smart city will mean in implementation.

Where are we Now?

The technology is here for smart cities, but should we be implementing this technology at scale yet? At the 2019 Institute of Electrical and Electronics Engineers (IEEE) Smart City Conference in Kansas City, technical panels detailed new methods for scaling smart city applications and integrating various data sets, improving technical smart city capabilities at a rapid pace. Yet, one of the themes that emerged in the plenary sessions in Kansas City was that answering the the call for technical improvements would not be sufficient to increase the deployment, utilization, and optimization of smart city applications. The reason? These are not merely technical problems, but socio-technical ones, and the rapid pace of technological improvement has in many ways outpaced our ability to manage that technology. While cities may have large networks of infrastructure and computers, they are not merely machines. The policy and governance questions around smart cities, which are still largely unanswered, may be as likely as technical ones to delay, or even derail, the benefits of smart cities.

Even in some large cities, IT governance may still be maturing. City Chief Information Security Officers are a relatively new invention, if they can be afforded at all. Many cities still employ IT professionals in civil service job titles that date back to the earliest introduction of computers into city government. Even the managerial capability to contract for modern IT systems, let alone the ability to evaluate their construction or assess their safety, is sometimes poorly developed. The fact that some cities lack the organizational or institutional capability to effectively implement, manage, contract for, or evaluate smart city goods and services offered by vendors may not prevent them from pursuing such projects.

Even in some large cities, IT governance may still be maturing.

Smart city deployments are almost always done in deep cooperation with the private sector. Do we trust these companies to have the greater good of citizens first in their mind? How they calculate risk and return on investment are naturally different. Indeed, companies have not just the right, but the fiduciary responsibility, to walk away from sectors, markets, or products that don't offer

strong outlooks for profits; however, cities do not have that luxury. There may be profitable smart city implementations that are technically feasible, but that violate some other concern that cities take seriously, like privacy, equity, accountability, or transparency.

Do our city leaders have the education or staff expertise to stand up to the technology firms? Do they have the financial backing or market position to do so? Do our city leaders have the technical support from state, federal, or non-profit partners to ask technology firms the hard questions about the economics and safety concerns of smart implementations? In many cities, unfortunately, the answer is no.

Much of the existing literature around smart cities has a utopian feel. It is certainly true that smart city applications can reduce costs in some cases, improve efficiency in some cases, and collectively improve urban service delivery and quality of life. However, like all technologies, smart city technologies are largely agnostic to whether they are implemented well, ethically, economically, safely, or with accountability.

What is a Smart City?

As researchers from the Brookhaven National Lab observed in 2000:

A vision of the city of the future has been presented—one that rests on the integration of science and technology through information systems. A future that will require a re-thinking of the relationships between government, city managers, business, academia and the research community. The title of this vision is Smart Cities.[6]

This observation sets the stage for our study of smart cities.

Our definition does not stray much from Hall et al's. A smart city uses information and communication technologies to increase operational efficiency and effectiveness, share information with the public, and improve the quality of services. To achieve these aims, cities deploy technology across various parts of city infrastructure. These technological systems will use sensors to collect data about the environment and city operations, centralized and distributed or embedded computing power to process that data, and actuators to manipulate urban infrastructure and adjust city operations. In this sense, the smart city transforms the city into a large socio-technological system (or a system of such systems) that "senses, thinks and acts."[7]

But this wide-scale implementation of technology introduces challenges in risk transfer, liability, citizen protection, data management, and citizen consent.

Managing Liability in Smart Cities

Cities and other organizations use insurance to decrease the risk burden of everything from natural disasters to accidents. Cyber insurance, however, is still an evolving market. The cyber insurance market lacks reliable data that can predict loss, especially in the public sector.[8] Partly because of the lack of data, insurance carriers face difficulty in pricing and underwriting, and they often closely limit the kind of coverage offered.

Not only is the cyber insurance market just beginning to mature, the more mature parts (like insurance for data breaches) are focused almost exclusively on traditional business IT systems—those responsible for data storage, transmission, and analysis. Smart cities, however, feature an explosion of cyber-physical systems in sectors from transportation, to water systems, to lighting, to parking, in which computers do not merely store and manipulate data, but collect data through sensors and manipulate the physical world through actuators of various types. Thus, the places in which cyber insurance has recently grown in value are for applications very different than the ones presented by smart cities. Increasingly, cyber insurance will be required for all sorts of physical systems which previously were not controlled by computers.

However, even if the insurance market evolves to cover physical systems, a number of important, open questions remain:

- In a highly technical environment that increases risk from cyber attacks or other technology-related issues affecting citizen services, how will insurers react?
- Will cities be able to offload as much risk as they need to for safe operations?
- Will insurers be able to reasonably price the risk of the shutdown of huge municipal systems (like transit systems) the way they are currently able to price the risk of breaches of Personally Identifiable Information (PII)?
- When a computer-controlled system fails, will such losses be viewed as losses under traditional property and casualty insurance or under cyber insurance?
- If an attack can't be attributed, or is attributed to a state actor, will cyber insurance coverage still pay out?[9]

The possibility that city infrastructure could be used by malicious actors for their own purposes raises further questions about liability for damages. IBM X-Force

research group found that many of the vulnerabilities that helped enable the October 2016 Mirai attacks remain in smart city devices.[10] The Mirai botnet used insecure IoT devices with default passwords to perpetuate a massive distributed denial of service (DDoS) attack on multiple targets.[11] Smart city technology would massively increase the amount of IoT devices deployed across the world; ensuring their security would be paramount to preventing criminal and offensive attacks.

The potential of having a city's "smart" infrastructure used in a cyberattack, particularly as a result of poor security practices or management, that targets victims across the world may expose a city to liability claims. So far, much of the discourse around liability for IoT-powered attacks has rested with the manufacturer; in a smart city implementation, where these devices are likely to be customized and/or integrated with other systems, liability exposure could increase.[12] In that case, is the city a victim or an accessory-by-neglect to the crime?

Furthermore, there is already a strong debate over whether a city can or should pay the ransom if its systems were affected by ransomware. Beyond the argument over the effectiveness of paying the ransom in the first place—many attackers are not sophisticated enough to actually decrypt what they encrypted[13]—cities have to deal with the moral conundrum of paying criminals from taxpayer funds.[14] In a smart city, it could be about getting back basic services like transportation or lighting, which changes the calculus by changing the level of consequence.

Citizen engagement and trust is critical in any smart city deployment, and issues of citizen consent pose a real challenge for the smart city concept. The success of the smart city model relies on the participation of citizens en masse, and many of the technologies are passive collectors, meaning that citizens do not actively opt-in. How can citizens give consent for smart city adoption? There is a huge education piece to this puzzle, first of all, and regardless if citizens are educated or not, it will be difficult, if not impossible, to turn services off for some citizens and on for others.

Relatedly, smart city implementations and other technological projects will often be done as pilot projects or phased implementations because resources are not available for major upfront capital investments. Thus, to paraphrase William Gibson, the future will arrive, it just won't be evenly distributed.[15] In a world in which the future is not evenly distributed, how will cities decide what areas and neighborhoods get smart applications first? In some cities it will be driven by questions of economic development, in others by the presence of certain industries or institutions (like universities). However it seems unlikely that it will start in the poorest or most in need areas in many cities. Thus, the explosion of smart cities and smart city projects will also create a vast set of questions about ethics and equity.

Data Ownership and Management

The focus on public-private partnerships in smart cities is the result of both technical expertise being resident in such companies and the fact that companies often create unique funding models to avoid forcing cities to make major upfront capital investments for the sensors, actuators, and computing platforms that make up the Internet of Things. This requires the companies to make up for such funds in alternative models of "monetization"[16] that may include selling smart city data to third parties or keeping data as proprietary information. These new business models could create problems around privacy, transparency, accountability, and other democratic values.

These new business models could create problems around privacy, transparency, accountability, and other democratic values.

Part of what should make citizens concerned is the question of data ownership and management. Most smart city implementations are done through cooperation between the private and public sectors. In most pilot programs, the private sector retains control over the data and leases it to the city, but in a mature program, the city should own the data for its services.[17]

However, if these conditions are achieved, several important questions remain:

- If the city owns and controls the data, where is the benefit for the private sector?
- Will the advantageous pricing offered today survive in that model?
- Can cities take advantage of these services if that kind of pricing is not continued?
- And if it isn't, will cities feel pressure to cede control over their data or share it with the private sector in a way that puts the security of its citizens at risk?

These questions get to the heart of the last concept discussed: consent. Forward-leaning cities such as New York, Amsterdam, and Barcelona have started talking about fundamental digital rights for their citizens,[18] but do those rights extend to data held by private companies? These arrangements have yet to be worked out. Other cities, like Seattle and Dallas, have begun to incorporate such concerns in their organizational structures by creating a Chief Privacy Officer position for the city or utilizing a non-profit structure to do community engagement.[19]

Even within cities, the question over data control and governance will be tricky. Data owners or the business unit (or agency) leaders that own an application typically decide how data can be used.[20] In a smart city environment, this decision must be tied to both the method of collection and purpose of the system, which will require technical expertise. This process is an added expense that will need to be integrated into any smart city deployment. Additionally, the elements of city government that support these business unit leaders—specifically those that provide legal counsel and support the purchase of insurance—will need to be involved in this decision-making as well. In many cases, data will be a valuable asset to a city[21] and will have to be treated as such.

What are we Protecting?

Data

The data collected in smart city applications varies across almost every possible spectrum and includes among the most sensitive personal data, as well as largely mundane and uninteresting data. Pressure readings in water mains, wind speed data from environmental monitors, and light level readings from smart lighting applications are the kinds of large-scale environmental data collections in some smart city applications that seem relatively innocuous and unconcerning and probably largely are. This data is valuable for adjusting city services for efficiency, and it poses little threat from breach or exposure. However, many smart city applications will collect information that is tied to individual users, their devices, their locations, and other sensitive information.

Smart parking applications or automated license plate readers will not just collect user license plate numbers, but they will tie that license plate to geocoded data about where it was collected. This is prototypical surveillance data, and often users will not have any option to opt in or opt out. Even seemingly less invasive applications, like city-provided free Wi-Fi hotspots or Bluetooth connections, could collect unexpected user data, like data from an embedded medical device that automatically connects to open Wi-Fi to upload telemetry. Are cities prepared to safely store logs filled with device information on citizens pacemakers, and would the pacemaker owners feel comfortable with this? Would the citizens even know?

Part of the challenge here is that we are consistently adding more and more devices to the environment, and so the data privacy concerns are broader than just data collection, and they increasingly include data collation across disparate and unconnected datasets. Datasets that will be, in the case of the smart city, owned and protected by either the municipality or their vendors. Cities are, in many cases, not currently prepared for the task of warehousing the vast amounts of data that smart city applications will produce—in terms of both the logistics of holding such data and the defensive agility to protect such data. Historically, cities have collected and stored a lot of sensitive data, but they did so largely at a human scale. The automation of collection platforms, the increasing sensitivity of data (because of technologies like geocoding and facial recognition), and the use of data to actually change physical city operations through actuators on infrastructure systems (vastly increasing the importance of data protection, and particularly data availability and integrity) means the new data protection challenge for cities is different in both scale and type.

Services

Smart city systems collect data to improve the effectiveness and efficiency of city services. These technologies can add to the span of delivery, save energy, fill gaps, add customization to offerings already provided, or enable new applications developed based on the data gathered. Once these digitally enabled services become the default, however, citizens and city officials alike will depend on them.

Once that happens, cities will face the same challenge as all critical infrastructure providers: high uptime requirements. High uptime requirements make updating systems more difficult because infrastructure often needs to be taken offline to be updated. With this concern in mind, city networks must be designed for resiliency and segmented appropriately to prevent attacks from spreading from system to system and to enable administrators to update systems regularly.

Additionally, systems must be designed to "fail usable." While failing safely or failing securely are common themes in engineering discussions of fault tolerance, even in terms of urban infrastructure and smart cities, failing to a usable state is less commonly explored or discussed.[22] The comedian Mitch Hedberg once joked, "I like an escalator man, because an escalator can never break, it can only become stairs."[23] Smart city applications–like Hedberg's escalator–will have to remain usable in some form if their digital componentry or network connections fail.

...The city must have a manual backup or usable setting that is automatically engaged upon system failure.

If essential city services are digitized—parking meters that are tied to phone applications, for example—and the application driving the service fails, the city must have a manual backup or usable setting that is automatically engaged upon system failure. City street lights controlled by motion sensors, for example, should default to "on" if the control system fails. An illustrative example of not "failing usable" was the ransomware infection on the payment kiosks of the San Francisco Municipal Transit Authority (SFMTA) light rail system. Because there was no manual back up, the system was faced with serious challenges, and the

city ultimately decided to let customers ride for free for several days while they reimaged all the systems in the payment kiosks.[24]

Citizens

There is a fundamental question that has yet to be answered: to what degree are cities responsible for the safety of their citizens? Some cities (and countries)[25] consider the digital security of their citizens to be just important as the physical security of their citizens, but this is a new and still frontier idea. There is still more work to be done on how much protection a city should and can provide, and to whom it provides protection. For example, is protection provided only to citizens of the city, or does it extend to those who work in it and those who travel to it?

Smart cities technology can improve the quality of services provided to citizens, but it will also introduce a considerable amount of additional digital risk to citizens, their data, and the services that are provided to them.

Should we even Bother?

With all of these concerns, then, should we even bother with smart city technology? The answer has to be yes. The increasing urbanization of the world's population, environmental concerns, and budget challenges demand that we do. But we need to do it safely.

Doing smart cities safely will cost more money in the short term. That is the reality. Such technology will ultimately usher in monetary savings and benefits for the larger community and the environment, but not as much as if systems were installed without the necessary security features and design. These features are necessary, and installing smart city technology without a security mindset and tooling raises too many risks. It is time to dedicate resources to answering the tough questions that go along with the benefits of technological innovation.

This economic reality—that a responsible and safe smart city is more (perhaps much more) expensive than just implementing smart technology immediately—must also be balanced against one of the more important realities of cities in the current era: that cities are struggling for resources. In the United States, cities are facing a series of important financial hurdles. Cities often face declining budgets or revenues,[26] shrinking state and/or federal support,[27] increasing pension obligations,[28] and ultimately more financial uncertainty.[29] Thus, at a time when we would prefer cities to be investing in making smart applications safer and more secure, they will often be in a financial situation that makes such investments much harder to justify. This resource challenge exacerbates the mismatch between city contracting capabilities and needs and the differing bottom lines and goals of cities and their vendors.

There is further research needed in multiple areas to make smart cities a truly "smart" reality.

Some of these key questions have been identified in this paper, and others will continue to pop up over time as new devices, systems, applications, and functionalities are introduced in smart cities. Cities will have to answer some, but they will not be able to do so alone. Other organizations and individuals—federal and state government agencies, legislatures at all levels, academic and research institutions, private sector companies, technologists, ethicists, lawyers and courts, and stakeholder and community organizations—will all have to play a part in working with cities to understand what smart city implementations truly mean for society and how to make sure the benefit is an overall positive one. In that sense, the project of making smart cities safe, stable, secure, and sustainable will be a national and communal one as much as a municipal one.

We have made amazing progress on the technical questions around smart cities and smart city applications. However, the technical questions are not the only

ones we face. There are still areas of concern, each of which will include not individual questions but large portfolios of questions—ethical, financial, social, logistical, political, demographic, economic, bureaucratic, and otherwise—that are decidedly not technical.

That said, there is a series of broader functions that define what it is that cities provide and are expected to provide for the people who live in them, work in them, and visit them. These functions can manifest as services—fire or emergency response, snow removal, trash collection, or education—or aspects of community—social justice, safety, or urban development. Each of the following broad areas of expectations have implications for smart cities and public policy, and each raise both broad philosophical and ethical questions as well as narrower, practical questions. Below are some of those broad philosophical questions, along with a non-comprehensive sampling of more specific ones.

- **Sustainable Finance**: What business models and investment or pricing strategies will make smart cities feasible and sustainable?
    - Should vendors be able to offer lower-cost smart city implementations in exchange for owning or monetizing the collected data?
    - Will the city or the vendor be responsible for the cost of maintenance, sensor calibration, and/or maintaining stores of spare components?
    - What will the exploding cost of data storage and processing needs that come with smarter cities do to city budgets, and how will that balance with potential savings?
- **Social Justice**: How will the implementation, management, and automation processes of smart cities differentially impact various communities, constituencies, and stakeholders in the city, and what responsibilities do cities have to mitigate these impacts?
    - What neighborhoods will get pilot or phased smart city implementations first? Will it be those with most needs or those that contribute the most to the city tax base?
    - What populations—domestic violence victims, the homeless, and/or the elderly—will face what risks from automated personal data collection in smart city applications?
    - Should companies be given tax credits or incentives for installing smart city applications, and where does that funding come from?

- **Security and Safety**: Can cities and their partners (from vendors, to state and federal government agencies, to third sector partners) really secure the data and systems that are likely to come with smart city growth?
    - Are city network operators going to be able to effectively monitor the alarms on intrusion detection systems when the number of devices on their networks doubles, triples, or increases by a factor of 10?
    - Will smart city transportation applications fail over into a manual mode, or will computer failures on the systems mean that city transit grinds to a halt? (And would the city even still employ drivers or train operators to do the manual work if there was a failure like this?)
    - How resistant to flooding are the sensor networks that operate a city's smart parking infrastructure? Can such systems be installed in flood prone areas?
- **Effective Municipal Operations**: Can cities improve their cross-agency, cross-disciplinary, and cross-jurisdiction coordination, as well as their contracting and acquisition processes, sufficiently to make smart cities viable?
    - When fire departments respond to calls at facilities with smart city infrastructure, will they know what infrastructure is where, and will they know how to avoid damaging it in the course of firefighting?
    - When a driver crosses the line between two municipalities, will they need a second smart parking token or beacon, or will the systems in adjoining communities be interoperable?
    - When parking meter data can be used to show who parks at or around hospitals or medical service providers, will parking management officials recognize that data as sensitive and valuable?
- **Consequence and Liability Management**: When people are injured, killed, or otherwise negatively impacted by automated systems that are part of a smart city, will cities, the courts, the insurance industry, first responders, and others be able to reasonably manage the consequences,

understand the technologies and systems sufficiently to assign blame, and take steps to mitigate such negative impacts?

- When buggy code results in the derailment of a subway car, will the court system be able to parcel out blame and responsibility among the city transit agency, train operators, vendors and system integrators, hardware and software producers, and other key stakeholders?

- If tens of thousands of smart city devices from across a dozen cities are used to conduct denial of service attacks on a company across the globe, what is the city's responsibility?

- If algorithms determine that it is more efficient to send trains more often to some neighborhoods than others because of traffic volume, but some percentage—30, 50, or 70 percent—of the less-served neighborhoods are among the more accessible ones, could that violate the Americans with Disabilities Act?

Each of these broad research areas is underdeveloped but key to answering a broader question about the viability and sustainability of the smart city ideal. We have to answer many of these questions to get a sense of the kind of smart cities we will end up with. The initial impulse will be to pursue the strategy of implementing smart cities "fast" and "cheap." Answering these questions will be an important part of changing the strategy to push toward optimizing for "good" smart cities.

Notes

1 Crawford, Susan P. *Fiber: The Coming Tech Revolution and Why America Might Miss It*. New Haven: Yale University Press, 2018.

2 Krywyj, Danny. "Data-rich IoT: The Only Smart Solution to Aging Infrastructure." Smart Cities World. June 29, 2018. https://www.smartcitiesworld.net/opinions/opinions/data-rich-iot-the-only-smart-solution-to-aging-infrastructure-; Marshall, Paul. "Aging Infrastructure: How Municipalities Can Make Smart Upgrades with Community Support." American City & Country. July 19, 2017. https://www.americancityandcounty.com/2017/07/19/aging-infrastructure-how-municipalities-can-make-smart-upgrades-with-community-support/.

3 Geib, Claudia. "Smart Cities May Be The Death of Privacy As We Know It." Futurism. January 17, 2018. https://futurism.com/privacy-smart-cities; *Cyber Security A Necessary Pillar of Smart Cities*. Report. 2016. https://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf.

4 Schneier, Bruce. "Opinion: Why It's so Easy to Hack Your Home." CNN. August 15, 2013. https://www.cnn.com/2013/08/14/opinion/schneier-hacking-baby-monitor/index.html.

5 Cui, Lei, Gang Xie, Youyang Qu, Longxiang Gao, and Yunyun Yang. "Security and Privacy in Smart Cities: Challenges and Opportunities." *IEEE Access* 6 (July 11, 2018): 46134-6145. doi:10.1109/access.2018.2853985.

6 Hall, Robert E., B. Bowerman, J. Braverman, J. Taylor, H. Todosow, and U. Von Wimmersperg. *The Vision of A Smart City*. Report. Brookhaven National Laboratory. Paris, France: 2nd International Life Extension Technology Workshop, 2000.

7 Schneier, Bruce. "The Internet of Things Will Be the World's Biggest Robot." Schneier on Security. February 4, 2016. https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html.

8 Friedman, Sam. "Demystifying Cyber Insurance Coverage." Deloitte Insights. February 23, 2017. https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html.

9 Ross, Andrew. "Mondelez Vs. Zurich: How Watertight Is Cyber Insurance Coverage?" Information Age. January 25, 2019. https://www.information-age.com/cyber-insurance-coverage-mondelez-zurich-123478253/.

10 Leonard, Matt. "Smart Cities Vulnerable to Easy Attacks on Unsecured Connected Apps." GCN. August 10, 2018. https://gcn.com/articles/2018/08/10/smart-city-security-vulnerabilities.aspx.

11 Fruhlinger, Josh. "The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet." CSO Online. March 09, 2018. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

12 Brown, Scott, General Counsel, BlueVoyant. Telephone interview by author. March 24, 2019.Also see for example:Norton Rose Fulbright. “Legal Implications of DDoS Attacks and the Internet of Things (IoT)” Data Protection Report. December 5. 2016. https://www.dataprotectionreport.com/2016/12/legal-implications-of-ddos-attacks-and-the-internet-of-things-iot/AndInternet Society. “IoT Security for Policy Makers” Internet of Things. April 19, 2018. https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

13 Mathews, Lee. "Why You Should Never Pay A Ransomware Ransom." Forbes. March 09, 2018. https://www.forbes.com/sites/leemathews/2018/03/09/why-you-should-never-pay-a-ransomware-ransom/#40b492221753.

14 Blinder, Alan, and Nicole Perlroth. "Hard Choice for Cities Under Cyberattack: Whether to Pay Ransom." The New York Times. March 29, 2018. https://www.nytimes.com/2018/03/29/us/atlanta-cyberattack-ransom.html; Kozloski, Matthew. "Cities Must Pay For Cybersecurity, Not Ransoms." Hartford Courant. October 22, 2018. https://www.courant.com/opinion/op-ed/hc-op-kozloski-west-haven-cyber-hack-20181022-story.html.

15 Maharajh, Robert. "The Future Has Arrived." Medium. May 24, 2016. https://medium.com/not-evenly-distributed/the-future-has-arrived-fed56cec3266.

16 McBride, Kurtis. "Monetizing Smart Cities: Framing the Debate." Centre for International Governance Innovation. March 28, 2018. https://www.cigionline.org/articles/monetizing-smart-city-data.

17 Sanders, Organizer: Jennifer Sanders Jennifer, Executive Director and Co-Founder, Dallas Innovation Alliance. Interview by author. February 20, 2019.

18 Lindsey, Nicole. "Smart Cities Begin to Embrace Digital Rights for Personal Privacy and Data Protection." CPO Magazine. December 18, 2018. https://www.cpomagazine.com/data-privacy/smart-cities-begin-to-embrace-digital-rights-for-personal-privacy-and-data-protection/.

19 Brazel, Rosalind. "City of Seattle Hires Ginger Armbruster as Chief Privacy Officer." Tech Talk. July 11, 2017. https://techtalk.seattle.gov/2017/07/11/city-of-seattle-hires-ginger-armbruster-as-chief-privacy-officer/; Sanders, Organizer: Jennifer Sanders Jennifer, Executive Director and Co-Founder, Dallas Innovation Alliance. Interview by author. February 20, 2019; Miller, Hugh, Chief Information Officer (CIO), Dallas, and Girish Ramachandran, Chief Technology Officer (CTO), Dallas. Interview by author. February 20, 2019; Duong, Steven, Associate Vice President of Design Planning at AECOM. Interview by author. February 19, 2019.

20 Askham, Nicola. "What Data Governance Roles Do You Need to Make Your Data Quality Initiative a Success?" Experian PLC. April 28, 2014. https://www.experian.co.uk/blogs/latest-thinking/data-and-innovation/what-data-governance-roles-do-you-need-to-make-your-data-quality-initiative-a-success/.

21 "The World's Most Valuable Resource Is No Longer Oil, but Data." The Economist. May 06, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

22 Godschalk, David R. "Urban Hazard Mitigation: Creating Resilient Cities." Natural Hazards Review 4, no. 3 (July 15, 2003): 136-43. doi:10.1061/(asce)1527-6988(2003)4:3(136); Harmon, Robert R., Enrique G. Castro-Leon, and Sandhiprakash Bhide. "Smart Cities and the Internet of Things." 2015 Portland International Conference on Management of Engineering and Technology (PICMET), August 2015. doi:10.1109/picmet.2015.7273174.

23 “Escalator,” YouTube video, posted by "mrburgy," March 7 2012, https://www.youtube.com/watch?v=7n1ryH3igKc.q7MIcN0A.

24 Holland, Kristen. "Update on SFMTA Ransomware Attack." San Francisco Municipal Transportation Agency. November 28, 2016. https://www.sfmta.com/blog/update-sfmta-ransomware-attack; News Staff. "San Francisco Transit Agency Recovers From Ransomware Attack." Government Technology State & Local. November 28, 2016. http://www.govtech.com/security/San-Francisco-Transit-Agency-Recovers-From-Ransomware-Attack.html.

25 Brown, Geoff, Chief Information Security Officer (CISO), New York City. Interview by author. July 26, 2018; National Cyber Security Strategy 2016 to 2021. Report. November 1, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

26 Urahn, Susan K. "The Local Squeeze: Falling Revenues and Growing Demand for Services Challenge Cities, Counties, and School Districts." The Pew Charitable Trusts. June 2012. https://www.pewtrusts.org/en/research-and-analysis/reports/0001/01/01/the-local-squeeze; Pagano, Michael A., and Christopher W. Hoene. "City Budgets in an Era of Increased Uncertainty." Brookings. July 18, 2018. https://www.brookings.edu/research/city-budgets-in-an-era-of-increased-uncertainty/.

27 Urahn, Susan K. "The Local Squeeze: Falling Revenues and Growing Demand for Services Challenge Cities, Counties, and School Districts." The Pew Charitable Trusts. June 2012. https://www.pewtrusts.org/en/research-and-analysis/reports/0001/01/01/the-local-squeeze.

28 Krouse, Sarah. "The Pension Hole for U.S. Cities and States Is the Size of Germany's Economy." The Wall Street Journal. July 30, 2018. https://www.wsj.com/articles/the-pension-hole-for-u-s-cities-and-states-is-the-size-of-japans-economy-1532972501.

29 Pagano, Michael A., and Christopher W. Hoene. "City Budgets in an Era of Increased Uncertainty." Brookings. July 18, 2018. https://www.brookings.edu/research/city-budgets-in-an-era-of-increased-uncertainty/.

NEW AMERICA