NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DIGITAL INFRASTRUCTURE'S CONNECTION BETWEEN CITIZENS AND THE CULTIVATION OF HOMELAND SECURITY TERRAIN

by

Noah R. Valero

December 2019

Thesis Advisor:	Rodrigo Nieto-Gomez
Second Reader:	Shannon A. Brown

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE DIGITAL INFRASTRUCTURE'S CONNECTION BETWEEN CITIZENS AND THE CULTIVATION OF HOMELAND SECURITY TERRAIN	**5. FUNDING NUMBERS**
6. AUTHOR(S) Noah R. Valero	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The purpose of this research is to investigate the shift of the homeland security landscape in response to rapid urbanization and integration of technology in cities. Governments and municipalities are rushing toward the utilization of advanced technologies to solve challenges dealing with urban expansion and the increase of high-tech threats. Privacy concerns and vulnerabilities in associated "smart city" design are becoming apparent and related to the adoption of new security measures. This thesis answers the question: How will the transformation of Homeland Security terrain, influenced by smart city infrastructure, affect how governments deliver services and security to citizens? The effects are revealed through the use of a comparative analysis between Singapore and Denmark, highlighting the governmental composition, social dynamics and policy approaches involved with smart city development. The comparison discloses that the effectiveness and implementation of a smart city design in part depends on the level of collaboration, training, and policy formulation in security planning that occurs among public-private, academic and citizen stakeholders. The results suggest that stakeholders should be involved from the beginning in smart city planning. Their initial involvement allows for security and privacy issues to be mitigated beforehand. It also encourages the public's trust of government services that are delivered in an advanced technological city environment.

14. SUBJECT TERMS interoperability, e-government, smart cities, digital communities, public-private, big data, terrain, digital ecosystem, smart grid, e-planning, e-democracy, e-participation, open data, open government, black swan attacks, smart healthcare, wireless, network, trust, privacy, security, smart city framework, internet of things, autonomous, e-readiness, urbanization, standardization, e-governance, collaboration	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

DIGITAL INFRASTRUCTURE'S CONNECTION BETWEEN CITIZENS AND THE CULTIVATION OF HOMELAND SECURITY TERRAIN

Noah R. Valero
Lieutenant, United States Navy
BS, Embry-Riddle Aeronautical University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2019

Approved by: Rodrigo Nieto-Gomez
Advisor

Shannon A. Brown
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this research is to investigate the shift of the homeland security landscape in response to rapid urbanization and integration of technology in cities. Governments and municipalities are rushing toward the utilization of advanced technologies to solve challenges dealing with urban expansion and the increase of high-tech threats. Privacy concerns and vulnerabilities in associated “smart city” design are becoming apparent and related to the adoption of new security measures. This thesis answers the question: How will the transformation of Homeland Security terrain, influenced by smart city infrastructure, affect how governments deliver services and security to citizens? The effects are revealed through the use of a comparative analysis between Singapore and Denmark, highlighting the governmental composition, social dynamics and policy approaches involved with smart city development. The comparison discloses that the effectiveness and implementation of a smart city design in part depends on the level of collaboration, training, and policy formulation in security planning that occurs among public-private, academic and citizen stakeholders. The results suggest that stakeholders should be involved from the beginning in smart city planning. Their initial involvement allows for security and privacy issues to be mitigated beforehand. It also encourages the public’s trust of government services that are delivered in an advanced technological city environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

3Vs	volume, variety, and velocity
ACLU	American Civil Liberties Union
ANPR	automatic number plate recognition
APT	advanced persistent threat
ASEAN	Association of South East Asian Nations
BDA	Big Data Analytics
CCTV	closed circuit television
CERTs	Computer Emergency Response Teams
CfCS	Danish Centre for Cyber Security
CMCA	Computer Misuse and Cybersecurity Act of 2017 enacted by Singapore's parliament
CPS	Cyber-Physical Systems
Datailsynet	Data Protection Agency of Denmark
DDIS	Danish Defense Intelligence Service
DDoS	Distributed Denial of Service
eCitizen	person in a country that uses electronics to access e-government services
E-government	electronic government
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FIP	Fair Information Practices
GPS	Global Positioning System
IC	intelligence community
ICCPR	International Covenant on Civil and Political Rights of 1966 enacted by Denmark's parliament
ICE	Immigration and Customs Enforcement
ICT	information and communications technology
ISAC	information sharing and analysis center
ISAO	information sharing and analysis organizations
ISP	Internet service provider
IT	information technology

MIT	Massachusetts Institute of Technology
MND	Ministry of National Development
NCP	National Computerization Plan
Next Gen NBN	Next Generation Nationwide Broadband Network
NITP	National Information Technology Plan
OAPEC	Organization of Arab Petroleum Exporting Countries
OPM	Office of Personnel Management
PAP	People’s Action Party
PDPA	Personal Data Protection Act of 2012 enacted by Singapore’s parliament
PII	Personally Identifiable Information
PolCam	police cameras
SCP	State and City Planning
UCGM	Urban Community Grids Management

I. INTRODUCTION

A. RESEARCH QUESTION

This thesis answers the question: How will the transformation of Homeland Security terrain, influenced by "Smart City" infrastructure, affect how government deliver services and security to citizens?

B. PROBLEM STATEMENT

"Smart Cities" are defined by William Eggers and John Skowron as "physical assets networked via sensor technology that generate streams of valuable data."[1] Houbing Song et al. points out that the aforementioned relies on a complex architecture that supports the interconnection among hardware, software, sensors, information, meters and advanced technology.[2]

Song et al. reports that smart cities interlink Information and Communications Technology (ICT) with Cyber-Physical Systems (CPS) in an urban environment, enabling machines to communicate, coordinate, and regulate infrastructure, promote the delivery of services, and provide city governance to enhance the well-being of citizens.[3] Song et al. emphasizes that smart cities by design serve the purpose of providing economic and social sustainability by managing resource consumption, reducing pollution, and optimizing city functions around an urban community's needs and values.[4]

Song et al. explains that smart cities help in the following ways. First, they support security by coordinating city lighting and surveillance devices to help prevent crime.[5]

[1] William Eggers and John Skowron, *Forces of Change: Smart Cities* (New York, NY: Deloitte Touche Tohmatsu Limited, 2018), https://www2.deloitte.com/insights/us/en/focus/smart-city/overview.html.

[2] Houbing Song, Stefano S. Bregni, Ravi Srinivasan, Tamim Sookoor and Sabina Jeschke, *Smart Cities: Foundations and Principles* (New York: John Wiley & Sons, Incorporated, 2017), 3.

[3] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 2.

[4] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles,* 3.

[5] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 5.

Energy consumption by the public is reduced when smart grid technologies are employed to control and manage the balance between renewable energy and fossil fuels.[6] The mobility of businesses and citizens is enhanced by smart cities coordination of geographic information and transportation modes that help reduce pollution, traffic congestion, and noise.[7] Smart city network technology increases access to education for all social classes to help communities develop new skills, and adapt to job markets and an evolving economy.[8] Smart cities encourage smart governance by synchronizing and expanding political participation and online public services to residents.[9]

Song et al. alleges that part of the problem with smart cities is that they are not adequately equipped to defend against data breaches, or have an adequate design architecture that integrates technologies in order to prevent issues with network functionality, inefficiencies and failures.[10] Kathryn Stephens defers to security consultant Tony Flick's statement that "Smart Grid development has become a 'gold rush' to get government money, but when industry rushes new technologies to market, they are more likely to be flawed and vulnerable."[11] Fixing these problems by accelerating the advancement of security measures is the first step in preparing smart cities for the protection of citizens.

Digital communities require a secure environment safeguarded by a homeland security terrain capable of protecting the distribution of public services in the form of healthcare, energy, transportation and law enforcement. However, the problem of inadequate homeland security measures is due to the rapid integration of technology in

[6] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 5.

[7] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 5.

[8] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 6.

[9] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 6.

[10] Song, Bregni, Srinivasan, Sookoor and Jeschke, *Smart Cities: Foundations and Principles*, 10.

[11] Kathryn Stephens, *U.S. Smart Grid Security: How Are We Doing*? (Smithfield, VA: National Security Cyberspace Institute, 2011), http://www.nsci-va.org/WhitePapers/2011-10-19-SmartGrid%20Security-Stephens.pdf.

cities that are creating vulnerabilities within the cyber-physical domain related to shortfalls in interoperability, resource allocation, and standardization.

In addition, these homeland security landscape problems also stem from deficiencies in public-private collaboration, information sharing, and the absence of a comprehensive policy for a smart city framework. Solving these problems is difficult because it requires complex public-private planning and agreement of policies, strategy, and the retrofitting of security design features that are compatible between old and new technologies without negatively affecting civil liberties.

Insufficient protective measures and vulnerabilities in smart cities are creating national security concerns. For example, in 2007, the President's Council of Advisors on Science and Technology raised awareness about the national security and critical infrastructure vulnerabilities of weak network access points for hackers to exploit, potential "black swan" attacks, and the overlapping of outdated architecture's susceptibility to failure from natural disasters.[12] According to the Project Grey Goose Report on Critical Infrastructure, "There have been at least 120 instances of successful attacks, some of which are documented in the report and date back to 2001."[13] The Project Grey Goose Report on Critical Infrastructure goes on to say that "state and/or non-state sponsored hackers from the Russian Federation of Independent States, Turkey, and China as the main threats to targeting and hacking into energy providers and other critical infrastructure networks."[14] The report anticipates a dramatic increase in attacks as the U.S. critical infrastructure domain incorporates more wireless and IP-based systems.[15]

The trust and privacy of citizens are as vital as national security when it comes to the usage of technology for the access of public services. For example, the automation

[12] John H Marburger et al., Leadership Under Challenge: Information Technology R&D in a Competitive World. An Assessment of the Federal Networking and Information Technology R&D Program (Washington, DC: White House, 2007), https://apps.dtic.mil/dtic/tr/fulltext/u2/a474709.pdf.

[13] Kelley J. Higgins, "Spike In Power Grid Attacks Likely In Next 12 Months," Informa PLC Informa UK Limited, February 19, 2010, https://www.darkreading.com/vulnerabilities---threats/spike-in-power-grid-attacks-likely-in-next-12-months/d/d-id/1132982.

[14] Higgins, "Spike In Power Grid Attacks Likely In Next 12 Months."

[15] Higgins, "Spike In Power Grid Attacks Likely In Next 12 Months."

and connectivity of Smart Healthcare systems provide remote virtual assistance and services to patients.[16] Cyber criminals are capable of penetrating medical devices and information systems by using ransomware and software for the collection of personal health information.[17] The compromise of citizen's privacy in smart cities can cause a lack of trust in public institutions; rendering public services unusable.[18]

The sharing of information between government and industry is critical for ensuring the protection of smart communities. Several presidential policies have been enacted since the Clinton Administration to encourage information sharing between government and the private sector.[19] From these policies the Information Sharing and Analysis Centers (ISAC) and Information Sharing and Analysis Organizations (ISAO) were established for the purpose of "exchanging threat, vulnerability and intrusion information" on a voluntary basis between government and industry.[20] However, companies engage in strategic interactions to prevent leakages of information to avoid negative marketing campaigns in order to avoid losing market share value and to maintain a competitive advantage within their sector.[21] The lack of information sharing and cooperation between government and industry makes it difficult for security agencies to effectively assess and respond in real time to threats within the smart city domain.

Smart cities in other countries are currently in advance stages of development. They are demonstrating various strategies and lessons learned in how government plays a role in providing security and access to public services in an evolving digital ecosystem. The U.S.

[16] Mohamad Amin Hasbini et al., *Smart Cities Appeal and 15 Things That Should Not Go Wrong* (n.p.: securingsmartcities.org, 2017), https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-15-things-v1.3.pdf.

[17] Mohamad Amin Hasbini et al., *Smart Cities Appeal And 15 Things That Should Not Go Wrong*.

[18] National Science and Technology Council, *The National Privacy Research Strategy* (Washington, DC: Whitehouse, 2016), https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf.

[19] Meilin He, Laura Devine, and Jun Zhuang, "Perspectives on Cybersecurity Information Sharing Among Multiple Stakeholders Using a Decision-Theoretic Approach," *Risk Analysis* 38, no. 2 (February 2018): 215, https://doi.org/10.1111/risa.12878.

[20] He, Devine and Zhuang, "Perspectives on Cybersecurity Information Sharing Among Multiple Stakeholders Using a Decision-Theoretic Approach," 216.

[21] He, Devine and Zhuang, "Perspectives on Cybersecurity Information Sharing Among Multiple Stakeholders Using a Decision-Theoretic Approach," 221.

can use smart city strategies from cities outside the U.S. as a model for solving its challenges in finding a comprehensive strategy for public-private collaboration, public-private information sharing, technology integration and a smart city framework.

C. LITERATURE REVIEW

The literature review calls attention to the potential benefits and vulnerabilities that come from the restructuring of the homeland security environment around technology, services, information and human behavior. Numerous scholarly, governmental, and peer-reviewed publications exist annotating the difficulties evolving in response to the convergence of technology, society, and homeland security climate. The majority of the literature focuses on the troubles facing the political and legal terrain. To further the research and analysis efforts in this thesis, the following categories were selected: checks and balances, citizen's right to privacy, electronic government (e-government) and big data in relation to "Smart City" infrastructure.

1. Checks and Balances

There have been numerous studies to investigate the concept of checks and balances. Some scholars argue that the separation of powers by legislative function impels three branches of government in the balancing of power, therefore preventing tyranny.[22] According to Robert Pushaw, the federalists believed that the separation of powers "preserv [es] liberty by checking and balancing governmental authority in support of protecting the rule of law."[23] Some political theorists, like M. J. C. Vile, claim that checks and balances are based on the separation of agencies (executive, legislative, and judicial branches), each of which carries distinct sets of values, interests, and procedures with internal mechanisms that inherently prevent the rise of a "single all-embracing agency of government."[24]

[22] Richard Albert, "The Separation of Higher Powers," *SMU LAW REVIEW* 65, no. 1 (July 2012): 69, https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1407&context=lsfp.

[23] Robert Jr. Pushaw, "Justiciability and Separation of Powers: a Neo-Federalist Approach." *Cornell Law Review* 81, no. 2 (January, 1996): 502, https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2592&context=clr.

[24] M. J. C. Vile, *Constitutionalism and the Separation of Powers. 2nd ed*. (Indianapolis: Liberty Fund, 1998), 16–18, Liberty Fund, Inc.

Others claim that a system of checks of balances is part of a greater social contract where voters forgo some liberties in exchange for government's protection of people's rights. Hints towards governmental checks and balances are conveyed in Aristotle's political theory.[25] He describes how the constitution is an agreement between citizens and politicians for "organizing the offices of the city-state" [26] for the purpose of establishing laws through institutions for the "common advantage" of all citizens.[27] Michael Warren notes that in the 18th century, Charles Secondat, Baron de Montesquieu's theory of separation of powers served as the cornerstone for James Madison's drafting of the U.S. Constitution and the embedding of a system of checks and balances as the essential component for safeguarding the people's liberty.[28]

Daron Acemoglu, James A Robinson, and Ragnar Torvik conducted research on the concept of "equilibrium checks and balances" and identified a political scale that can be influenced by the elite or poor voters of a democratic society.[29] They assert that well organized elite and poor groups of voters undermine checks and balances through lobbying and bribing to influence the reduction of "politician's rents" and to encourage politicians to act in the groups favor at the expense of the majority of voters.[30] The National Bureau of Economic Research group found that judicial checks and balances ensure greater economic and political freedom by preventing the legislature and executive branch from acting in self-interest.[31]

[25] Fred Miller, "Aristotle's Political Theory in The Stanford Encyclopedia of Philosophy," Metaphysics Research Lab, Stanford University, November 7, 2017, https://plato.stanford.edu/archives/win2017/entries/aristotle-politics/.

[26] Miller, "Aristotle's Political Theory in The Stanford Encyclopedia of Philosophy."

[27] Miller, "Aristotle's Political Theory in The Stanford Encyclopedia of Philosophy."

[28] "America's Survival Guide," Mill City Press, Inc., Accessed July 11, 2019, http://www.americassurvivalguide.com/montesquieu.php.

[29] Daron Acemoglu, James A Robinson, and Ragnar Torvik, "Why Do Voters Dismantle Checks and Balances?" (working paper, National Bureau of Economic Research, 2011), 37, https://www.nber.org/papers/w17293.pdf.

[30] Acemoglu, Robinson, and Torvik, "Why Do Voters Dismantle Checks and Balances?"

[31] Acemoglu, Robinson, and Torvik, "Why Do Voters Dismantle Checks and Balances?"

Some constitutional scholars, like Frank Vibert, claim that contemporary unelected technocrats and institutions form a new kind of separation of powers system at the domestic and international levels.[32] The assertion is that unelected groups provide information to citizens in a democratic society that is superior to the factual information provided by governments; this allows citizens to check politicians' motives and enable voters to influence policy formulation in an alternative way.[33]

An increasing area of literature offered by scholars like Albert Meijer have studied the social, political and technical interactions in the handling of data as a key factor in the balancing of power between communities, companies, and politicians in smart city governance.[34] Meijer studied public governance of smart cities and discovered that the power balancing mechanisms depend on the combining of social, political and technical features encourages citizen involvement in decision-making about digital infrastructure development.[35]

In a 2007 congressional hearing before the Judiciary Committee, representatives argued that warrantless surveillance authorized through the Foreign Intelligence Surveillance Act fundamentally defeats the check and balance constraints, violating U.S. citizen's right to privacy and denying their right to search and seizure.[36]

Liberal theorists, like Paul Starr, claim that democratic liberalism infers a society supported by a constitution that outlines a system of checks and balances.[37] According to

[32] Frank Vibert, *The Rise of the Unelected: Democracy and the New Separation of Powers* (Cambridge, UNITED KINGDOM: Cambridge University Press, 2007), 166, ProQuest.

[33] Vibert, The Rise of the Unelected: Democracy and the New Separation of Powers, 167.

[34] Albert Meijer, "Datapolis: A Public Governance Perspective on 'Smart Cities,'" *Perspectives on Public Management and Governance* 1, no. 3 (August, 2018): 195–206, https://doi.org/10.1093/ppmgov/gvx017.

[35] Meijer, "Datapolis: A Public Governance Perspective on 'Smart Cities,'" 204.

[36] Warrantless Surveillance and the Foreign Intelligence Surveillance Act : the Role of Checks and Balances in Protecting American's Privacy Rights. Pt. II : Hearing before the Committee on the Judiciary, House of Representatives, 110 Cong., 1st Sess., September 18, 2007, 1.

[37] Paul Starr, "Liberalism and the Discipline of Power," in Freedom's Power: The True Force of Liberalism (Basic Books, April 2007), 18, Princeton.edu.

Starr, institutional mechanisms and participation in elections helps prevent state power from becoming despotic.[38]

From a global perspective, well known international relations theorists use neorealism to describe how power is checked and balanced between nations within the international community through security or military expansion in the interest of the state at the expense of personal liberties.[39] Many experts contend, however, that neorealism falls short in explaining the influence individuals have for reigning in the government's power in a liberal democracy.[40]

2. Privacy

Many scholars throughout history have conducted ample research on the subject of privacy. In 1978, Richard Posner wrote from an economic theory perspective of privacy that "the strongest defenders of privacy usually define the individual's right to privacy as the right to control the flow of information about him."[41]

Some scholars, like Alexandra Rengel, assert that privacy is an inherent value that is comparable to love, friendship and trust.[42] Edward Bloustein equates the protection of a person's personality with the protection of a person's privacy, independence, and dignity.[43]

Rengel claims that privacy and security are a balancing act to protect American society as a whole. The assumption is that in an Internet age the accumulation of personal

[38] Starr, "Liberalism and the Discipline of Power,"18.

[39] Charles W. Kegley, Shannon L. Blanton, *World Politics: Trend and Transformation, 13th ed.* (Wadsworth: Cengage Learning, 2010), 70, https://hostnezt.com/cssfiles/internationalrelations/World%20Politics%20Trend%20and%20Transformation%202010%20to%202011%20Edition%20By%20Charles%20William%20Kegley.pdf.

[40] Starr, Liberalism and the Discipline of Power," in Freedom's Power: The True Force of Liberalism, 17.

[41] Richard A. Posner, "An Economic Theory Of Privacy," *AEI Journal On Government And Society* (2008): 20, https://doi.org/10.1017/cbo9780511625138.

[42] Alexandra Rengel, *Privacy in the 21st Century* (Leiden: Martinus Nijhoff Publishers, 2013), 32, ProQuest.

[43] Rengel, Privacy in the 21st Century, 32.

data by public-private organizations may be used as justification for compromising individual privacy in support of national security.[44] In other words, the security of society as a whole benefit when individuals give up a share of their privacy.[45]

France Belanger and Robert Crossler conducted privacy attitudes research. They found that the usage of fair information practices (FIP) in the management of people's information mitigated online users' privacy concerns to the point that they were more likely to provide personal information and less likely to take precautions in protecting their privacy.[46] They also found that trust for Internet users to have a mediating effect on [consumer's] relationship between privacy concerns and willingness of online transactions."[47]

In 2017, Susan Athey, Christian Catalini, and Catherine Tucker introduced the "Digital Privacy Paradox" experiment at Massachusetts Institute of Technology (MIT) was conducted on a group of students concerning digital privacy choices.[48] The experiment revealed in Athey, Catalini and Tucker's research state in part that, "whereas people say they care about privacy, they are willing to relinquish private data quite easily when incentivized to do so."[49]

[44] Rengel, Privacy in the 21st Century, 61.

[45] Rengel, Privacy in the 21st Century, 61.

[46] France Bélanger and Robert E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* 35, no. 4 (December 2011): 1021, https://doi.org/10.2307/41409971.

[47] Bélanger and Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," 1021.

[48] Susan Athey, Christian Catalini, and Catherine Tucker, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," (working paper, National Bureau of Economic Research, 2017), 1, https://www.nber.org/papers/w23488.pdf.

[49] Athey, Catalini, and Tucker, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk."

It has recently been demonstrated by Reinhold Kesler, Michael Kimmer, and Patrick Schulte that mobile app developers over time increasingly adopt personally intrusive data collections tactics towards its users.[50]

In 2012, a congressional hearing was held on the implications of facial recognition technology on privacy and civil liberties.[51] From an individualistic standpoint, Maneesha Mithal argued that a citizen's facial images can be used by unrestrained public-private entities to uniquely identify unsuspecting persons for profit or prosecution.[52] Furthermore, government representatives argue that facial images are the key to unlocking personal information in part: social network profiles, names, and a person's movements.[53] Facial images allow strangers to access tons of personal information in seconds about citizens from a distance.[54]

3. Electronic Government

Technology is playing a greater role in service functions extended by government, bridging the divide between public-private sectors when it comes to the intermediate distribution of public services. However, the literature does little in addressing the importance of human behavior's role in effective e-government implementation. The literature reveals areas of opportunities and barriers generated by e-government platforms.

Christopher Reddick describes electronic government (e-government) as the usage of Information-Communication Technology (ICT) to facilitate cheaper and efficient access

[50] Reinhold Kesler, Michael F. Kummer, and Patrick Schulte, Chloe Reichel, "Mobile Applications and Access to Private Data: The Supply Side of the Android Ecosystem," (working paper, Centre for European Economic Research, 2017), 19, https://dx.doi.org/10.2139/ssrn.3106571.

[51] What Facial Recognition Technology Means for Privacy and Civil Liberties Hearing Before the Subcommittee on Privacy Technology and the Law of the Committee on the Judiciary United States Senate, 112 Cong. (2012), https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.

[52] H.R., What Facial Recognition Technology Means for Privacy and Civil Liberties.

[53] H.R., What Facial Recognition Technology Means for Privacy and Civil Liberties.

[54] H.R., What Facial Recognition Technology Means for Privacy and Civil Liberties.

of online services to the public, businesses, and governmental entities.[55] Tax preparation and healthcare are examples of web-based tools used to enhance the lives of citizens.

Some scholarly writings examine the barriers that are limiting public access to these online programs. Mary Schmeida and Ramona McNeal found that the digital divide can be attributed to inequalities in Internet access, technological skills, and psychological barriers among the poor, young (Millennials) and elderly (Baby Boomers).[56] They go on to say that these inequalities can be limited with government policies and programs.[57] Schmeida and McNeal used a "multivariate regression analysis and individual level data"[58] to answer the question, "how successful have government efforts been to bring underserved Americans online to Medicare and Medicaid public health insurance information?"'[59] Additionally, their research found that government's role can enhance the public's access to health insurance programs by providing Internet based information on Medicare eligibility criteria, enrollment guidelines, and public health service centers.[60]

Scholars write about factors confronting the effective installation of e-government amenities and essential components for the shaping of citizens' behavior and of a digital ecosystem. The existence and availability of technology for public use is not enough to attract citizen interaction; some individuals need encouragement to entice their participation.

[55] Christopher G. Reddick, *Comparative E-Government* (New York: Springer Science+Business Media, LLC, 2010), 5, https://doi.org/10.1007/978-1-4419-6536-3_5.

[56] Mary Schmeida and Ramona McNeal, "Bridging the Inequality Gap to Accessing Medicare and Medicaid Information Online: An Empirical Analysis of E-government Success 2002 through 2010," *In E-Government Success around the World: Cases, Empirical Studies, and Practical Recommendations*, ed. J. Ramon Gil-Garcia, (Hershey, PA : Information Science Reference, an imprint of IGI Global, 2013), 62, doi:10.4018/978-1-4666-4173-0.ch004.

[57] Schmeida and McNeal. "Bridging the Inequality Gap to Accessing Medicare and Medicaid Information Online: An Empirical Analysis of E-government Success 2002 through 2010," 72.

[58] Schmeida and McNeal. "Bridging the Inequality Gap to Accessing Medicare and Medicaid Information Online: An Empirical Analysis of E-government Success 2002 through 2010," 60.

[59] Schmeida and McNeal. "Bridging the Inequality Gap to Accessing Medicare and Medicaid Information Online: An Empirical Analysis of E-government Success 2002 through 2010," 61.

[60] Schmeida and McNeal. "Bridging the Inequality Gap to Accessing Medicare and Medicaid Information Online: An Empirical Analysis of E-government Success 2002 through 2010," 61.

Kurtz, Sagamore, and Cole investigated techniques used to increase citizen participation in online government services of tax preparation and vehicle registration at the state level. They assert that cost effectiveness from e-government services rely on increased usage. They address the efficacy of the government's encouragement of citizens' usage of e-government services based on human behavior and state marketing investments made.[61] They found that taxpayers' behavior towards the usage of online services can be encouraged with marketing that ensures web service convenience, ease, and safety.[62]

Liu's and Yuan's case study assessed "Urban Community Grids Management (UCGM) effects on local governments across three cities (Beijing, Shanghai and Wuhan).[63] They found factors that were effective for finding ways to enable the delivery of public services and improved communications between government and citizens.[64] According to Shuhua Monica Liu and Qianli Yuan, factors that lead to the success of e-government amenities fell under two categories: technical and organizational.[65] They claim that accessibility, quality, and efficient communications across dynamic societal and technological boundaries are favorable to the electronic environment.[66] The success of e-government is contingent on the quality of leadership, management, and process modification around the needs of citizens, which build the value users are looking for.[67]

[61] Jennifer A. Kurtz, Roland J. Cole, and Isabel A. Cole, *Politics, Democracy and E-Government: Participation and Service Delivery* (Hershey PA : Information Science Reference, 2010), chap. 2, https://doi.org/10.4018/978-1-61520-933-0.ch002.

[62] Kurtz, Cole and Cole, Politics, Democracy and E-Government: Participation and Service Delivery, 34.

[63] Shuhua M. Liu, and Qianli Yuan. "Urban Community Grids Management in Metropolitan China: A Case Study on Factors Contributing to Mobile Governance Success." *In E-Government Success around the World: Cases, Empirical Studies, and Practical Recommendations*, ed. J. Ramon Gil-Garcia, 145, (Hershey, PA : Information Science Reference, 2013), https://doi.org/10.4018/978-1-4666-4173-0.ch008

[64] Liu and Yuan. "Urban Community Grids Management in Metropolitan China: A Case Study on Factors Contributing to Mobile Governance Success," 149.

[65] Liu and Yuan. "Urban Community Grids Management in Metropolitan China: A Case Study on Factors Contributing to Mobile Governance Success," 160.

[66] Liu and Yuan. "Urban Community Grids Management in Metropolitan China: A Case Study on Factors Contributing to Mobile Governance Success," 148.

[67] Liu and Yuan. "Urban Community Grids Management in Metropolitan China: A Case Study on Factors Contributing to Mobile Governance Success," 149.

Trust is a powerful factor that significantly affects e-government implementation. According to Gabriel Puron-Cid, "trust is one of the most influential factors for e-government success."[68] He adds "the literature points out different types of trust related to e-government adoption: trust of internet, trust of government, perceived usefulness of technology, perceived quality of e-government services, and disposition to trust."[69] These types of trust help form the dimensions from which to observe the interaction between citizens and government.[70]

Once online public services are implemented and available for citizens' use, they must be measured for quality to ensure follow-on sustainment and improvement. Measuring e-readiness is significant for the evaluation of the effectiveness of e-government implementation, in the assessment of citizen interactions with online services, and for the management of digital ecosystems.

Lei Zheng writes about e-readiness assessment practices, focusing on the features, issues, and problems from a local city's perspective.[71] In this effort, Zheng designs a bottom up approach for prescribing a customizable blueprint for assessing different phases of e-government development and readiness of cities, countries or government agencies.[72] Zheng's approach analyzes the political, regulatory, organizational, cultural, communication, and technological factors in a government's ability to use Internet and communications technology (ICT) for growing as economy and promoting the public's

[68] Gabriel Puron-Cid, "Trust Measures for Implementers of E-Government Adoption: A Confirmatory Factor Analysis." In *E-Government Success around the World: Cases, Empirical Studies, and Practical Recommendations*, ed. J. Ramon Gil-Garcia, (Hershey, PA : Information Science Reference, an imprint of IGI Global, 2013), 79–104, https://doi.org/10.4018/978-1-4666-4173-0.ch005

[69] Puron-Cid, Gabriel. "Trust Measures for Implementers of E-Government Adoption: A Confirmatory Factor Analysis," 94.

[70] Puron-Cid, Gabriel. "Trust Measures for Implementers of E-Government Adoption: A Confirmatory Factor Analysis," 81.

[71] Lei Zheng, "Developing E-government Readiness Factors: A Bottom-Up Approach," In *E-Government Success around the World: Cases, Empirical Studies, and Practical Recommendations,* ed. J. Ramon Gil-Garcia (Hershey, PA : Information Science Reference, an imprint of IGI Glob, 2013) 133, https://doi.org/10.4018/978-1-4666-4173-0.ch007.

[72] Zheng, "Developing E-government Readiness Factors: A Bottom-Up Approach," 132.

well-being.[73] Furthermore, according to Zheng, "e-readiness assessment can be an effective tool to carry out planning, monitoring and evaluation of the initiatives toward Information Society in general and e-Government in particular," which help promote smart city governance.[74]

4. Big Data

Big data publications highlight the mixture of technology and public services resulting in the massive accumulation of data. Marie Lowman emphasizes that big data can be used as a significant driver for change in methods of collection, management, and analysis of information.[75]

In recent years there has been growing interest in the volume, velocity, and variety (3Vs) dimensions of big data management. Doug Laney draws our attention to how 3Vs in an information age are pertinent to a common understanding in the public-private collaboration and management of growing complex data.[76]

Ossi Ylijokil and Jari Porras traced the evolution of the big data definition.[77] They conclude that there are currently 17 different definitions of big data. They assert that many of the definitions are inconsistent because technical and usage aspects are mixed and, additionally, that current definitions are limited in accounting for security and privacy attributes.[78]

[73] Zheng, "Developing E-government Readiness Factors: A Bottom-Up Approach," 133.

[74] Zheng, "Developing E-government Readiness Factors: A Bottom-Up Approach," 133.

[75] Marie Lowman, *A Practical Guide to Analytics for Governments : Using Big Data for Good* (Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017), 134, ProQuest.

[76] Doug Laney, "3D Data Management Controlling Data Volume Velocity and Variety," Gartner (blog), February 6, 2001, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

[77] Ossi Ylijoki and Jari Porras, "Perspectives to Definition of Big Data: A Mapping Study and Discussion," *Journal of Innovation Management* JIM 4, no. 1 (May 2016), 79, https://doi.org/10.24840/2183-0606_004.001_0006.

[78] Ylijoki and Porras, "Perspectives to Definition of Big Data: A Mapping Study and Discussion," 79.

In 2019, an executive survey was conducted about how big data is being used in business transformation.[79] Surprisingly, 95 percent of business executives point to cultural and organizational barriers, instead of technical problems, as reasons preventing the full adoption of big data in companies.[80]

Song et al. in their research concluded that big data analysis is the key for innovation and allow citizens to act on new insights to help reformat city infrastructure and change how people behave in order to achieve a smarter world.[81]

Micael Stonebraker argues in a panel discussion forum conducted by Communications of the ACM that predictive models and big data analysis algorithms are built by humans with a variety of biases, a situation which can create a world of deception if not carefully improved and managed over time.[82]

Some experts, like Patrick Park, argue that big data analytics fail most of the time because industry perceives the indiscriminate massive collection and analysis of data is good in general without tying it to specific objectives and meaningful results.[83] Furthermore, he asserts that the success of big data analysis relies on a combination of humanities and engineering to create human value and should be the priority.[84]

Won Kim, Ok-Ran Jeong, and Chulyun Kim assert that the human element is overlooked when it comes to big data analysis which is needed in determining the meaning

[79] Thomas H. Davenport and Randy Bean, "Big Data and AI Executive Survey 2019," New Vantage Partners, January 2019, https://newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf.

[80] Davenport and Bean, "Big Data and AI Executive Survey 2019."

[81] Song, Smart Cities: Foundations and Principles, 26.

[82] CACM Staff, "Big Data," *Communications of the ACM* 60, no. 6 (May, 2017): 25, https://doi.org/10.1145/3079064.

[83] Patrick H. Park, *Big Data War : How to Survive Global Big Data Competition First edition* (New York, New York 222 East 46th Street, New York, NY 10017 : Business Expert Press, 2016), 8, ProQuest.

[84] Park, *Big Data War : How to Survive Global Big Data Competition*, First edition, 8.

behind the data, prioritizing what data should be analyzed, and in conducting big data analysis process.[85]

D. RESEARCH DESIGN

The aim of this research is to discover solutions to challenges linked to smart cities influence over the transformation of homeland security and public service delivery to citizens. This thesis first examines the overarching privacy and security challenges to homeland security derived from the implementation of smart city strategies.

I will qualitatively analyze information related to those challenges using a comparative case study approach to highlight differences and similarities on how those challenges are managed between countries that are in the process of putting smart city strategies into practice.

The two case studies chosen are Singapore and Denmark, because of their unique governmental configurations and differing attitudes towards the notion of privacy and security. Moreover, both are considered advanced and innovative countries that have taken different paths toward the implementation of smart city concepts, and both states share similar issues.

This thesis will not explore the theory behind how specific types of technologies function. Instead it will highlight the effectiveness of policies, public-private organizations' roles, and practices that may help fill gaps within the United States homeland security terrain influenced by the adoption of technology within urban communities.

E. CHAPTER OUTLINE

The thesis will be separated into five chapters. Chapter I will annotate the problem, and present the thesis question, significance of the question, and the literature review. The

[85] Won Kim, Ok-Ran Jeong and Chulyun Kim. "A Holistic View of Big Data," In *Big Data: Concepts, Methodologies, Tools, and Applications,* ed. Information Resources Management Association (Hershey, Pennsylvania : Information Science Reference, 2016), https://doi.org/10.4018/978-1-4666-9840-6.ch004.

literature review will outline publications related to smart security, big data, e-government, and smart standards. This Chapter will conclude with my research design and thesis outline.

Chapter II will shine a spotlight on challenges facing homeland security's ability to adapt and apply adequate protective measures to digital communities. The factors contributing to these challenges include, public-private information sharing, information-communications technology standardization, management of big data, and privacy.

Chapter III will compare U.S. and foreign smart city cases to reveal strengths, weaknesses and various approaches to the governance over citizens and online government societies.

Chapter IV will provide the results from the information provided in the comparative case studies and analysis discussed in Chapter III.

Chapter V will provide a synopsis and recommendations of the research conducted with regards to homeland security's environmental challenges and opportunities being created for the community's usage of online government services.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CHALLENGES FOR HOMELAND SECURITY'S ADJUSTMENT TO A SMART CITY ECOSYSTEM

People are migrating from rural areas to cities, placing great stress on aging infrastructure and resources in cities around the world. In response, many countries are relying more on technology to manage limited resources while delivering government services and security to citizens.

This changes the way society interact within smart cities, how smart cities govern, and how personal information is used among communities, businesses, and government. Significant questions are being raised about the significant challenges with the integration of technology in cities which are changing the landscape of homeland security. Specifically, how should vast amounts of personal data be managed? What measures are needed to facilitate information sharing practices between government and private agencies in order to maintain citizens' privacy within a digital environment?

Chapter II calls attention to the leading challenges that delay cities from maximizing the full potential of a smart city ecosystem. Challenges are associated with big data management, information sharing in the public-private sector, privacy, and standardization. Additionally, this chapter attempts to illustrate related policy choices that have done more harm than good in the overall functioning of smart cities. This chapter also indicates a lack of coordination and citizen stakeholder involvement as underlying contributing factors to an incoherent smart city strategy.

A. BIG DATA MANAGEMENT

Big Data is known as big amounts of information accumulated as a result of society's interaction with smart cities information technology (IT) services.[86] Big data's value is maximized when a protected process includes both effective management and analysis principles.[87]

[86] Pethuru Raj and Anupama C. Raman, *Intelligent Cities : Enabling Tools and Technology* (Boca Raton, Florida: CRC Press, 2015), 299, https://doi.org/10.1201/b18561.

[87] Raj and Raman, *Intelligent Cities : Enabling Tools and Technology*, 288.

Today, big data analytics (BDA) allow for online information to be used to interpret people's behavior in the interest of identifying individuals and increasing the public's awareness of what precautions to take.[88] Businesses are able to gain immediate feedback on customer satisfaction to help forecast economic market changes.[89] Law enforcement conducts intelligent-policing with the usage of Close Circuit Television (CCTV), facial recognition software, cameras and GPS to reduce overall crime in urban areas.[90] Moreover, big data analytics is helping save lives in the healthcare industry. big data Analytics makes possible the 24-hr monitoring of babies in hospitals and the ability for healthcare professionals to respond to life-threatening conditions in real time.[91] However, there are issues that need to be addressed.

Big data has introduced a set of challenges related to the complex characteristics of data. Big data varies significantly between users and requires dynamic ways for it to be safeguarded by public-private organizations.[92] In the absence of big data management and infrastructure to support it; public-private organizations may be victimized by cyber intrusions. For example, in 2015, the U.S. Office of Personnel Management (OPM) was hacked, and millions of personal records and information stolen.[93] In a separate incident in 2015, healthcare company Anthem Inc. was hacked, leading to stolen patient medical ID numbers, income and contact information.[94]

[88] Bernard Marr, *Big Data Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance* (West Sussex, United Kingdom: John Wiley & Sons, Incorporated, 2015), 128, ProQuest.

[89] Marr, *Big Data Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance,* 109.

[90] Marr, *Big Data Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance,* 130.

[91] Marr, *Big Data Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance,* 136.

[92] Vincenzo Morabito, *Big Data and Analytics Strategic and Organizational Impacts* (Cham: Springer International Publishing, 2015), viii, https://doi.org/10.1007/978-3-319-10665-6.

[93] Tho H. Nguyen, *Leaders and Innovators : How Data-Driven Organizations Are Winning with Analytics*, Wiley and Sas Business Series (Hoboken: Wiley, 2016), 168, ProQuest.

[94] Nguyen, *Leaders and Innovators : How Data-Driven Organizations Are Winning with Analytics, Wiley and Sas Business Series*, 168.

B. PUBLIC-PRIVATE INFORMATION SHARING

The value of big data in an information age has precipitated the exponential production, and sharing of information facilitated by technology's role in smart societies. It is critical for smart cities to aide in the collaboration among stakeholders, owners, and operators in the forming of security measures around complex network environments.[95] Elaborate information and interdependencies of networks, societies, and agencies are confronted by pervasive threats to national security. Security agencies depend heavily on the information sharing practices in collaboration with federal, state, local and tribal entities.[96]

Smart ecosystems allow criminals to conveniently leverage online resources to inflict severe and costly damages on citizens. In order to respond effectively to these types of threats, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, which led to the establishment of 77 Fusion Centers.[97]

The purpose of fusion centers is to enable federal intelligence experts to relay classified information to law enforcement, emergency responders and critical infrastructure operators.[98] Fusion centers are meant to be a conduit for information sharing to flow both ways between public-private organizations.

There are significant problems impeding information sharing mechanisms.[99] Brian Jenkins, Andrew Liepman, and Henry Willis describe challenges that inhibit the sharing of

[95] Chirag Shah, *Collaborative Information Seeking The Art and Science of Making the Whole Greater than the Sum of All*, The Information Retrieval Series, 34 (Berlin, Heidelberg: Springer Berlin Heidelberg, 2012), ix, https://doi.org/10.1007/978-3-642-28813-5.

[96] Thomas E. McNamara, *Information Sharing Environment Implementation Plan*, ISE Implementation Plan (Washington, D.C: Office of the Director of National Intelligence, Program Manager, Information Sharing Environment, 2006) https://www.dni.gov/files/ISE/documents/DocumentLibrary/ise-impplan-200611_0.pdf.

[97] United States, Office of the Director of National Intelligence, *Domestic Approach to National Intelligence* (Washington, D.C.: Office of the Director of National Intelligence, 2016), https://www.dni.gov/files/documents/Newsroom/DomesticApproachtoNationalIntelligence.PDF.

[98] United States, Office of the Director of National Intelligence, *Domestic Approach to National Intelligence.*

[99] Brian M. Jenkins, Andrew Liepman, and Henry H. Willis, "Identifying Enemies among Us : Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing," Conference Proceedings, CF-317 (Santa Monica, CA: Rand Corporation, 2014).

information domestically between the FBI and law enforcement agencies.[100] Part of the problem is that the intelligence community (IC) currently operates without a unified approach towards intelligence operations.[101] Second, the FBI's role is directed towards the prevention of "high end" attacks and lacked the capacity in dealing effectively with cyber intrusions or detecting homegrown terrorists.[102] Third, information that is collected and combined by Fusion Centers is not shared laterally between other operation centers or police departments around the country.[103] The inability of security and law enforcement agencies in the sharing of information effectively and in a new digital age will hamper the progress needed in an evolving homeland security landscape.

Adding to the debate of information sharing practices, civil liberties pose concerns of the limits that exist in regards to collecting domestic information with the objective of ensuring a smart and secure urban environment.[104] According to the Constitution Project, violations to freedom of speech are likely to occur without proper regulations or oversight of law enforcement agencies.[105] At the same time, citizens' trust erodes when civil liberties are unprotected. Trust is vital because it affects security agencies reliance on society's assistance in counterterrorism or law enforcement intelligence operations.[106]

[100] Jenkins, Liepman, and Willis, "Identifying Enemies among Us : Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing," Conference Proceedings.

[101] Jenkins, Liepman, and Willis, "Identifying Enemies among Us : Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing," Conference Proceedings.

[102] Jenkins, Liepman, and Willis, "Identifying Enemies among Us : Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing," Conference Proceedings.

[103] Jenkins, Liepman, and Willis, "Identifying Enemies among Us : Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing," Conference Proceedings.

[104] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism* (Washington, D.C.: The Constitution Project, 2012, https://constitutionproject.org/pdf/fusioncenterreport.pdf.

[105] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[106] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

The Code of Federal Regulation #28, Part 23 forbids law enforcement agencies that are funded by the government from "collecting or maintaining personal information about individuals in criminal databases,"[107] except if there is "reasonable suspicion" that a person is part of some sort of criminal activity.[108] The determination of "reasonable suspicion" by law enforcement is based on a subjective decision which can be indiscriminately applied.[109] In 2012, the Constitution Project reported that counterterrorism trainers taught personnel at Fusion Centers to monitor the phones of Muslim academic groups and mosques to stop the infiltration of Sharia Law in the United States.[110]

Furthermore, fusion centers are able to access federal and state record databases, to gain personal data that includes drivers' licenses, insurance, credit reports, and phone numbers from illegitimate information brokers.[111] Fusion center experts use personal data to solve crime cases, but without addressing the potential intelligence gaps, this may lead to mistakes and result in falsely accusing certain individuals.[112]

In an effort to bridge the gap in information sharing between federal, law enforcement and the private sector; fusion centers are embedding private sector representatives within their facilities with access to personal information but without the proper clearances.[113] Nevertheless, there are minimal restraints for private companies from sharing customer information with fusion center databases or verifying their compliance

[107] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[108] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[109] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[110] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[111] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[112] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[113] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

with legal requirements in the handling of personal information.[114] Fusion centers are a significant component in the homeland security terrain that provide an essential conduit for public-private collaboration and for ensuring a secure digital environment. Smart ecosystems and civil liberties may be inadequately protected if fusion center dysfunctions in information sharing activities go uncorrected.

C. PRIVACY

Personal privacy of smart city residents is at risk of being jeopardized by the extensiveness of big data and the government's reliance on the sharing of personal information. The fourth amendment of the U.S. Constitution protects a citizen's right to privacy and affords them the option of keeping personal information from the public in order to remain anonymous.[115] However, in 2015, President Trump overturned a privacy rule that was enforced by the Federal Communications Commission (FCC), which no longer prevents internet service providers from sharing customer's online data with other companies.[116] Internet Service Providers (ISPs) supply online services to customers while concealing their ability of free access to their customers' online activity. Knowing how Internet Service Providers (ISPs) are using customer information from wireless services is important because it can be used to track a customers' location or, if mishandled, can lead to personal vulnerabilities for online consumers.[117]

The American Civil Liberties Union (ACLU) perceives smart cities as "surveillance cities," because the technology embedded within cities is viewed as a way of surveilling poor and colored parts of digital communities disproportionately.[118] For instance, Oakland California, a sanctuary city, collected license plate information routinely

[114] The Constitution Project, *Recommendations for Fusion Center Preserving Privacy & Civil Liberties while Protecting against Crime & Terrorism*.

[115] Pushaw, "Justiciability and Separation of Powers: A Neo-Federalist Approach."

[116] Alex Kang, "FCC Privacy Rule Repealed," The Regulatory Review, April 6, 2017, https://www.theregreview.org/2017/04/06/kang-fcc-privacy-rule-repealed/.

[117] Kang, "FCC Privacy Rule Repealed."

[118] Chad Marlow and Maryiam Saifuddin, "How to Stop 'Smart Cities' From Becoming 'Surveillance Cities,'" American Civil Liberties Union, September 17, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-stop-smart-cities-becoming-surveillance-cities.

on its residents and transferred it from the transportation department.[119] The transportation department then passed the license plate information to regional intelligence fusion centers and the U.S. Immigration and Customs Enforcement (ICE) agency to help track down undocumented immigrants.[120]

Additionally, citizens are nervous because of cities like San Diego have started to install smart street light systems called the "ShotSpotter network."[121] ShotSpotter networks contain LEDs and sensors that are able to recognize gunfire and alert the police in real time.[122] The concern of city residents is that the local government of San Diego will place them in locations based on law enforcement's personal biases such as high crime areas and poor, and colored city neighborhoods.[123]

Striking a balance between personal privacy and a smart city's incorporation of technology in the delivery of public services will require citizens to participate in city government so they can communicate their concerns to city managers on decisions pertaining to a smart city's effects on personal privacy.

D. STANDARDIZATION

Standardization in smart city development is critical to the design of information technology (IT), policy, and public-private organizations in the development of a smart city framework. Standards create a common perception and expectations of people, systems, or services.[124] Lawrence Busch asserts that society views previously formulated rules or systems to define what we deem as a model for the qualities of ethics and safety.[125]

[119] Sarah Holder, "The Shadowy Side of LED Streetlights," CityLab, March 8, 2018, https://www.citylab.com/equity/2018/03/their-lights-were-watching-odd/554696/.

[120] Sarah Holder, "The Shadowy Side of LED Streetlights."

[121] Sarah Holder, "The Shadowy Side of LED Streetlights."

[122] Sarah Holder, "The Shadowy Side of LED Streetlights."

[123] Sarah Holder, "The Shadowy Side of LED Streetlights."

[124] Lawrence Busch, *Standards : Recipes for Reality*, Infrastructures Series (Cambridge, Massachusetts: MIT Press, 2011), 2, ProQuest.

[125] Busch, *Standards : Recipes for Reality*, Infrastructures Series, 2.

He claims that standards can be "measured, tested, examined and revised."[126] Standardizing the concept of time during the U.S. industrial revolution in the 19th century allowed railroads to move materials and labor forces across the country on time, which brought economic prosperity to a significant portion of society.[127] A public-private agreement on the standards in the design of clocks and the interpretation of time in relation to a public train transport system created a reliable and valuable service to communities worldwide.

City planners, engineers and leaders have formed working groups over the last ten years in an attempt to address significant standardization concerns relevant to smart city development. The public-private consensus is that standardization is needed in the development of intelligent city architecture.[128] Smart city standardization can promote the efficiency of equipment, safety and public services under an umbrella of protection for people with minimal interoperable barriers.[129]

Standards can lead to efficient use of resources.[130] According to the National Institute and Standards Technology "sound interoperability standards will ensure that public and private sector technology investments are not wasted. Such standards enable diverse systems and their components to work together and to securely exchange meaningful information."[131] Furthermore, the institute envisions "large, integrated and complex systems [that] require different layers of interoperability."[132]

[126] Busch, *Standards : Recipes for Reality*, Infrastructures Series, 4.

[127] Busch, *Standards : Recipes for Reality*, Infrastructures Series, 91.

[128] Tobias Langenberg, Standardization and Expectations (Berlin, Heidelberg: Springer, 2006), 9, https://doi-org.libproxy.nps.edu/10.1007/3-540-28113-4, 9.

[129] Langenberg, Standardization and Expectations, 9.

[130] National Institute of Standards Technology (NIST). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0,* NISTIR 7628 (Washington, D.C.: White House, 2014), http://dx.doi.org/10.6028/NIST.SP.1108r3, 32.

[131] National Institute of Standards Technology (NIST). NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, 36.

[132] National Institute of Standards Technology (NIST). NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, 36.

III. CASE STUDIES: SINGAPORE AND DENMARK

This chapter compares the impacts of smart city concepts in connection to the delivery of public services, privacy and national security to the citizens of Singapore and Denmark. The expansion of national security measures in response to digital city operations are affecting the privacy of citizens in Singapore and Denmark. Comparing the methods in the implementation of smart city strategies in each country may reveal the elements that impact privacy and security of citizens.

The Singapore and Denmark are "developed countries" with advanced economies and infrastructure.[133] In terms of human development,[134] the populations of all three countries lead the world in the level of education completed by an average person, have a higher than average standard of living and live longer and healthier lives.[135] Moreover, all three countries are notable for demonstrating their innovative ability in the development of technological solutions for solving major societal problems. According to the 2018 Global Innovation Index, all three countries are in the top ten for creating an innovative environment through policies, institutions, and expertise who are capable of achieving greater economic output than most other countries.[136] However, this is where most similarities pertinent to this chapter end. Each country is unique in the way public services and security are provided via smart city strategies to improve the well-being of their society and how privacy is considered in related matters.

[133] World Population Review, "Developed Countries List 2019," World Population Review, October 4, 2019, http://worldpopulationreview.com/countries/developed-countries/.

[134] World Population Review, "Developed Countries List 2019."

[135] United Nations Development Programme, "*Human Development Index (HDI) | Human Development Reports*" (New York, NY: Creativecommons.org, 2019), http://hdr.undp.org/en/content/human-development-index-hdi.

[136] Cornell University, INSEAD, and the World Intellectual Property Organization, "*Global Innovation Index 2018: Energizing the World with Innovation*" (Geneva, Switzerland, by the World Intellectual Property Organization (WIPO), and in New Delhi, India, and by the Confederation of Indian Industry: Ithaca, Fontainebleau, and Geneva, 2018), 430, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018.pdf.

A. CASE STUDY: SINGAPORE

1. History and Origins of Singapore's Smart City Strategy

The beginnings of Singapore's smart city strategy were driven by its government's ability to overcome significant challenges stemming from its geography, limited living space and newfound independence.[137] These challenges increased unemployment, housing, water, and infrastructure problems.[138] Its struggles with these challenges are important for understanding the environmental and political dimensions that have sparked a nationally unified effort towards the usage of technology and expertise in accelerating its development.

Singapore's independence and political dynamics were shaped by its history with adversity caused by Japanese aggression during WWII, British colonialism in the early 20th century, and constant internal ethnic-group struggles.[139] In 1965, Singapore claimed its independence from Malaysia to become the Republic of Singapore.[140] Singapore's newfound independence set the stage for its political People's Action Party (PAP) to emerge and take control of its unicameral-parliament system for decades to come.[141]

Some claim that Singapore's government is democratic yet governs itself more like an autocracy. This outside perspective may have been originally shaped by Singapore's first Prime Minister Lee Kuan Yew and his draconian use of power.[142] In 2015, former Prime Minister Lee Kuan Yew died but his principles of what have been described as

[137] Greg Clark and Tim Moonen, *World Cities and Nation States* (Chichester, UK: John Wiley & Sons, Ltd, 2017), 192, ProQuest.

[138] Clark and Moonen, World Cities and Nation States, 192.

[139] "History of Singapore - Nations Online Project," Nationsonline.org, 2019, https://www.nationsonline.org/oneworld/History/Singapore-history.htm.

[140] Greg Clark and Tim Moonen, *World Cities and Nation States* (Chichester, UK: John Wiley & Sons, Ltd, 2017), 192, ProQuest.

[141] Nationsonline.org, "History of Singapore – Nations Online Project."

[142] Carlton Tan, "Lee Kuan Yew Leaves a Legacy of Authoritarian Pragmatism," *The Guardian*, March 23, 2015. World news, https://www.theguardian.com/world/2015/mar/23/lee-kuan-yews-legacy-of-authoritarian-pragmatism-will-serve-singapore-well.

pragmatic and authoritarian, still remain.[143] According to Carlton Tan, the People Action Party's (PAP) continue to apply Yew's principles in the manner of what Tan calls "calculated coercion" in order to keep the population happy for the purpose of maintaining its autocratic rule over Singapore.[144]

Additionally, Joshua Kurlantzick points out that the People's Action Party's (PAP) success in maintaining state control can be attributed to a few significant factors.[145] First, the People's Action Party's (PAP) makes slight adjustments in response to the public's sentiment that helps maintain its advantage over any type of political opposition.[146] Second, Kurlantzick states that the People's Action Party's (PAP) has instituted significant gerrymandering imposed against its political opposition.[147] And third, the People's Action Party's (PAP) has full control over resources and significant influence over the media in Singapore and leverage them in support of maintaining governmental control.[148]

Even though the political dynamics at play in Singapore were complicated at the time, its government was unified in its efforts towards aggressively advancing Singapore's overall national development. The People's Action Party (PAP) initially worked in solving its problems by leveraging its air transport, major shipbuilding, and oil refining industries in sustaining its economic growth from the 1970s through the 1990s.[149] Eventually Singapore moved its "labor intensive industries"[150] to other countries that were a part of the Association of Southeast Asian Nations (ASEAN) and "replaced them with high-technology production and a service-based economy."[151]

[143] Tan, "Lee Kuan Yew Leaves a Legacy of Authoritarian Pragmatism."

[144] Tan, "Lee Kuan Yew Leaves a Legacy of Authoritarian Pragmatism."

[145] Joshua Kurlantzick, "How Singapore's People's Action Party Continued Its 50-Year Reign," *The National*, September 24, 2015, https://www.thenational.ae/arts-culture/how-singapore-s-people-s-action-party-continued-its-50-year-reign-1.126824.

[146] Kurlantzick, "How Singapore's People's Action Party Continued Its 50-Year Reign."

[147] Kurlantzick, "How Singapore's People's Action Party Continued Its 50-Year Reign."

[148] Kurlantzick, "How Singapore's People's Action Party Continued Its 50-Year Reign."

[149] Nationsonline.org, "History of Singapore - Nations Online Project."

[150] Nationsonline.org, "History of Singapore - Nations Online Project."

[151] Nationsonline.org, "History of Singapore - Nations Online Project."

Singapore's government realized that future developmental planning would need to involve public-private stakeholders if it wanted to maintain its "political independence and economic" growth while concurrently mending its social-culturally fractured society.[152] To that end, Singapore's Ministry of National Development (MND) partnered with the State and City Planning (SCP) group to bring public and private key personnel together for the purpose of forming the "1971 Concept Plan."[153] The aim of the Concept Plan was to expand "Singapore's economic base, reduce unemployment, slow down the rate of population growth, and improve [its] standard of living."[154]

Unlike the United States, Singapore used a government led approach and a thirty-year outlook in their planning process that incorporated urban, social, and economic development policies.[155] Additionally, Singapore's parliament formed several smart city agencies and enlisted the help of private and educational experts from the beginning for the collaboration of smart city implementation.

2. Singapore Smart Infrastructure and Public Service Delivery

Singapore smart city plans evolved through multiple phases that focused initially on building the information technology and telecommunication architecture needed to achieve its objectives. Singapore's smart city and infrastructure was designed in six master-plans derived from its 1971 concept plan. The smart city master-plans were implemented in two phases.[156] The first phase took place from 1980 to 1992 which formed "The National Computerization Plan (NCP), National IT Plan (NITP), and IT2000"[157] together

[152] Koh Buck Song, "Liveable and Sustainable Cities: Common Challenges, Shared Solutions," in *WORLD CITIES SUMMIT CONFERENCE PROCEEDINGS 2014* (June 2014): 57*,* http://www.bufbd.org/images/selectedreports/2015/wcs14conf_proceedings_ebook_v2.pdf.

[153] Song, "Liveable and Sustainable Cities: Common Challenges, Shared Solutions," 56.

[154] Song, "Liveable and Sustainable Cities: Common Challenges, Shared Solutions," 57.

[155] Song, "Liveable and Sustainable Cities: Common Challenges, Shared Solutions," 57.

[156] Thiam Seng Koh, Sai Choo Lee, and Soh Tin Ho, *Information Communication Technology in Education: Singapore's ICT Masterplans, 1997–2008* (Singapore: World Scientific Publishing Co Pte Ltd, 2008), 8, ProQuest.

[157] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore's ICT Masterplans, 1997–2008 , 8.

formed a three step approach for advancing it’s national information communications infrastructure.[158] The first step was to computerize Singapore’s governmental departments and the delivery of its public services.[159] The second step emphasized the use of technology in the exchanging of data between government, businesses, and the public.[160] The third step involved the installation of national information technology (IT) infrastructure linking all “homes, office buildings, schools, and factories.” [161]

The next phase of Singapore’s smart city design centered on the delivery of government services using information technology. This phase of initiatives consisted of the Infocomm21, Connected Singapore, and iN2015 plans which were implemented from 2000 to 2006.[162] Once Singapore had the basic information technology and telecommunications infrastructure in place, it was able to provide electronic government (e-government) services to the public.[163] In addition, broadband capacity across Singapore was expanded to support the pervasiveness of “wireless,” “wired networks,” and “mobile services.”[164] Furthermore, the iN2015 plan sought to spread ultra-high speed and wireless broadband networks throughout Singapore to establish an “e-society,” “e-economy,” and to enable Singapore to become a global information-communications capital.[165]

[158] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[159] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[160] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[161] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[162] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[163] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[164] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

[165] Koh, Lee, and Ho, Information Communication Technology in Education: Singapore’s ICT Masterplans, 1997–2008 , 8.

Singapore's information-technology (IT) infrastructure and its vision for public service delivery[166] constructed a robust electronic-Government (e-government) service platform for its citizens.[167] Singapore's level of smart city preparedness in the offering of e-government services was driven by the aspects of access, information-communications infrastructure capacity, and in the arrangement of online services.

Improving the access, quality and efficiency of Singapore's new smart city platform were areas that helped encouraged the usage of public services provided to citizens. Singapore's smart infrastructure platform affords the majority of its citizens access to fast and efficient online information and the services necessary to communicate with its government, businesses, and communities.[168] In 2016, Freedom House reported that "91 percent"[169] of Singaporean families have access to broadband internet services.[170] Furthermore, "95 percent of homes and businesses"[171] have access to a "fiber-based Next Generation Broadband Network (Next Gen NBN)."[172] Singapore also offers free national "Wireless@SG" access at over "3,900 hotspots" to the public.[173]

The high quality and extensive public access to online government services encourages citizens to use its internet platform increasing the readiness and return on investment made towards smart city infrastructure. Furthermore, according to Toshio Obi and Naoko Iwasaki, Singapore ranked #1 in 2015 in World e-Government preparedness.[174] The evaluation of e-Government preparedness was measured in part by the deployment of

[166] N. C. Saxena, *The Singapore Public Service and National Development: Virtuous Cycles* (Singapore: Ministry of Foreign Affairs Singapore, 2012), 88, http://www.mfa.gov.sg/content/dam/mfa/images/media_center/MFA_CSC_UNDP_book/Virtuous_Cycles.pdf.

[167] Saxena, The Singapore Public Service and National Development: Virtuous Cycles, 96.

[168] Saxena, The Singapore Public Service and National Development: Virtuous Cycles, 95.

[169] Freedomhouse.org, "Singapore PARTLY FREE" (Washington, D.C.: Freedomhouse.org, 2018), https://freedomhouse.org/report/freedom-net/2018/singapore.

[170] Freedomhouse.org, "Singapore Partly Free."

[171] Freedomhouse.org, "Singapore Partly Free."

[172] Freedomhouse.org, "Singapore Partly Free."

[173] Freedomhouse.org, "Singapore Partly Free."

[174] Toshio Obi, *A Decade of World E-Government Rankings, Global E-Governance Series*, Volume 7 (Amsterdam: IOS Press, 2015), 1, ProQuest.

information-communications technology (ICT) infrastructure, "operations, management optimization, online services and the relationship between governments and their stakeholders."[175]

Singapore's eCitizen Portal is "a single access point to all government information and services on the internet"[176] and allows several government agencies to utilize the same resources in providing over 1,600 online services to its citizens.[177] The online services are known as "eTowns" and are grouped together into separate access points for its citizens, businesses, and government entities.[178] Part of the eTown services include healthcare, housing, transportation, education, security, and community development.[179]

3. Privacy Versus Checks and Balances in Singapore

Maintaining the privacy of online users in smart communities is becoming more difficult due to the lack of rules, oversight, and awareness in how personal information is managed in the virtual public sphere. The personal data collected in citizens interactions with e-government services has significant value for public and private organizations. Personal data in this context means "information relating to an identified or identifiable individual (data subject)."[180] Individuals' information is created or available in the form of online searches, photos, videos, social data, geo-location or identifiable information (police, health, financial…etc.).[181]

[175] Obi, *A Decade of World E-Government Rankings, Global E-Governance Series*, 4.

[176] Weiling Ke and Kwok Kee Wei, "Successful E-Government in Singapore: How did Singapore manage to get most of its public services deliverable online?" Communications of the ACM 47, no. 6 (June 2004), 96, https://doi.org/10.1145/990680.990687.

[177] Ke and Wei, "Successful E-Government in Singapore: How did Singapore manage to get most of its public services deliverable online?" 4.

[178] Ke and Wei, "Successful E-Government in Singapore: How did Singapore manage to get most of its public services deliverable online?" 2.

[179] Ke and Wei, "Successful E-Government in Singapore: How did Singapore manage to get most of its public services deliverable online?" 3.

[180] OECD, "*Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*" (Paris: OECD iLibrary, 2013), https://read.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en#page1, 7.

[181] OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value," 8.

Singaporeans have concerns about how their data is handled and used in relation to their privacy, but those concerns lack the level of enthusiasm needed to dissuade complacent online behavior. According to a 2016 KPMG privacy survey, 56 percent of Singaporeans "are either concerned or extremely concerned" when it comes to the "level of trust in [how] organizations [handle] their personal data."[182] Less than 55 percent actively "manage their social media privacy settings."[183] Less than 45 percent "regularly change username and passwords."[184] And less than 35 percent "examine privacy policies and cookie notifications."[185] This shows a significant contradiction when it comes to personal data concerns and complacency issues of Singaporean's usage of high-tech services. Such contradictions raise questions about what governments can do to improve awareness and education to mitigate complacency and safeguarding methods of personal data that the public can use.

Privacy is taken into consideration in Singapore's smart city strategy but is not a main priority. Unlike America's constitution, "Singapore's constitution does not contain any explicit right to privacy."[186] Nevertheless, the Parliament of Singapore has put a series of key regulations in place on how private organizations manage personal data and citizens' privacy. The Personal Data Protection Act of 2012 (PDPA), Computer Misuse and Cybersecurity Act (CMCA) and the Cybersecurity Act established a "national cyber framework"[187] for protecting critical information infrastructure and citizens' personal data against threats and potential private sector mishandlings of personal data.[188]

[182] KPMG, *Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line*, Report No. 134122-G (Switzerland: KMPG International, 2016), 36, p. 29 https://assets.kpmg/content/dam/kpmg/se/pdf/advisory/2016/se-Creepy-or-cool-report_web.pdf, 39, 36.

[183] KPMG, Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line, 9.

[184] KPMG, Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line, 9.

[185] KPMG, Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line, 9.

[186] James Gomez, Freedom Of Expression And The Media In Singapore (London: Article 19, 2005), 67, https://www.article19.org/data/files/pdfs/publications/singapore-baseline-study.pdf.

[187] Yuet M. Tham, "Singapore," in *The Privacy Data Protection And Cybersecurity Law Review Fifth Edition*, ed. Alan C. Raul (United Kingdom: Law Business Research Ltd, 2018), 287, https://thelawreviews.co.uk//digital_assets/b5f160ac-fb67-48da-be84-a085ee98b2f2/The-Privacy-Data-Protection-and-Cybersecurity-Edition-5.pdf.

[188] Tham, "Singapore," 287.

Although Singapore's government makes an effort in defending its citizens' privacy against the private sector, it does very little in restraining itself from accessing and using its citizens' personal data. This is because Singapore's parliament is exempted from major portions of its policies, like the Personal Data Protection Act.[189] This allows Singapore's government to force internet service providers to hand over personal data of their users[190] and in blocking certain public websites.[191] For example, "in 2013, Citizen Lab of the University of Toronto" discovered the Singapore government utilizes Bluecoat software, which has the capability to conduct surveillance of public applications like: Google, Twitter and Skype.[192] Singapore's police have the authority to "intercept online messages" and search and seize computers without a warrant in search of documents related to crimes involving online transactions.[193] Such exemptions give Singapore's government broad powers to exercise strict online censorship and control over the expression of its citizens when it comes to politics and religion.[194]

The security measures used by Singapore policymakers raises questions about the effectiveness of its checks and balance system. Singapore's constitution originated from the "Westminister model"[195] which includes a separation of powers system within three branches of government: the executive, legislative and judiciary.[196] However, over time Singapore's People's Action Party (PAP) have worked together in overriding power

[189] Terence Lee, "Singapore an Advanced Surveillance State, but Citizens Don't Mind," *Tech in Asia*, November 25, 2013, https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind.

[190] Lee, "Singapore an Advanced Surveillance State, but Citizens Don't Mind."

[191] Gomez, Freedom of Expression and the Media in Singapore," 68.

[192] PrivacyInternational.org, *The Right to Privacy in Singapore* (London: Privacyinternational.org, 2015), https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf., bullet 32.

[193] Gomez, Freedom of Expression and the Media in Singapore," 68.

[194] "Singapore: Space Narrows for Online News Media," *Human Rights Watch*, October 15, 2014, https://www.hrw.org/news/2014/10/15/singapore-space-narrows-online-news-media.

[195] Kevin T. Y. Lee, "The Evolution Of Singapore's Modern Constitution: Developments From 1945 To The Present Day," *Singapore Academy of Law Journal* 1 (1989): https://ssrn.com/abstract=626724.

[196] "The Rule Of Law And The Singapore Constitution," Supreme Court Singapore, April 25, 2019, https://www.supremecourt.gov.sg/news/events/magna/the-rule-of-law-and-the-singapore-constitution.

checking methods leading to its new label as a “dictatorial political system”[197] by overshadowing and silencing their political rivals.[198]

The separation of powers was unable to restrain Singapore’s government leaders because of their successful efforts in thwarting fair elections, freedom of expression, and stacking the political deck in favor of the People’s Action Party (PAP) in the wake of national economic success.[199] Singapore’s parliament has passed laws like the Sedition Act, to prevent online criticism.[200] In a similar manner it passed the Newspaper and Printing Presses Act and the Broadcasting Act, which permitted greater flexibilities in the licensing and regulation of the internet activities and organizations.[201] Some argue that despite Singapore’s government abuses of power, it maintains control over the nation by distracting its public with economic prosperity through “authoritarian capitalism.”[202]

4. Security

The privacy and personal information of citizens in smart communities are related and impact the level of trust needed for smart city sustainment. Singapore’s smart infrastructure, public services, and accumulation of data impacts how security and personal data protection is provided to its citizens. Singapore’s e-government platform and services generate tons of personal data that has to be protected and properly managed. When personal data is not adequately safeguarded, vulnerabilities emerge through the publicity of cyber-attacks making the safety of smart city services questionable.

Hacker and cyber criminals are taking advantage of the vulnerabilities within global information technology domains with sophisticated types of cyber-attacks. Spear Phishing,

[197] Tom Bailey, “How Singapore Married Dictatorship with a Market Economy,” *World Finance The Voice Of The Market*, July 16, 2015, https://www.worldfinance.com/special-reports/how-singapore-married-dictatorship-with-a-market-economy.

[198] Bailey, “How Singapore Married Dictatorship with a Market Economy.”

[199] Bailey, “How Singapore Married Dictatorship with a Market Economy.”

[200] Freedomhouse.org, *Freedom On The Net 2015 Singapore* (Washington, D.C.: Freedomhouse.org, 2015), https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Singapore.pdf.

[201] Freedomhouse.org, Freedom On The Net 2015 Singapore.

[202] Bailey, “How Singapore Married Dictatorship with a Market Economy.”

Distributed Denial of Service (DDos), and Advanced Persistent Threats (APTs) are types of trending cyber-attacks in the search for private data that are launched against individuals, companies, and government agencies.[203] According to Stephen Morgan, data breaches across the world will cost "$2.1 trillion" by [the end of] 2019."[204] The consequences of widespread cyber-attacks and vulnerabilities in all facets of societies worldwide have become too expensive to ignore.

Singapore has taken the initiative in confronting these types of pervasive cyber threats and related vulnerabilities. Singapore has instituted security applications and initiatives when it comes to the handling of personal information and public safety in cities.[205] In support of protecting individuals, Singapore has created smart city applications for its citizens to use when accessing online health, banking and other public services.[206] For instance, the National Digital Identity application allots users a single digital identity token for domestic or international transactions with any Singapore government agency for online public services.[207] This has reduced the risk of fraud and improved personal and network security for Singapore's city population.

Singapore is one of the best countries in preparedness when defending against digital theft in a growing smart city era. According to the Economist's Safe Cities Index

[203] INFOCOMM Development Authority Of Singapore, National Cyber Security Masterplan (Singapore, International Telecommunication Union (ITU), 2018), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Singapore_2013_AnnexA.pdf., p. 6.

[204] Steven Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," *FORBES*, January 17, 2016, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6eb950993a91.

[205] International Comparative Legal Guides (ICLG), *Singapore: Data Protection 2019* (London, United Kingdom: Global Legal Group, 2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore.

[206] Smart Nation and Digital Government Office, *Annex A Strategic National Projects for a SmartNation* (Singapore: Smart Nation and Ditigal Government Office, 2019), https://www.tech.gov.sg/files/media/media-releases/2017/08/Annex%20A%20StrategicNationalProjectsforaSmartNation.pdf.

[207] "Media Factsheet National Digital Identity," Government Technology Agency (GOVTECH SINGAPORE), 2018, https://www.smartnation.sg/docs/default-source/cos2018/national-digital-identity-factsheet.pdf.

2017 report, Singapore ranked second in terms of digital security and first in personal and infrastructure security.[208]

Singapore is empowering its civil servants with training in cyber threats and weaknesses. The introduction of a mandatory cyber security training course is currently provided by Singapore's Smart Nation and Digital Government Office for its public service employees.[209] In 2019, the training program encompassed "145,000 officers" across "16 ministries and over 60 statutory boards."[210]

The monitoring of Singapore's localities has significantly ramped up to help assist Singapore's police force in the reducing of crime. Singapore's law enforcement agencies have deployed the police camera installation initiative, Polcam 2.0 which was responsible for the installation of over "5,000" cameras within its smart city public areas which included homes, carparks, transport stations, and downtown areas.[211] According to Yi, the PolCam system has aided in solving over "2,300" crimes.[212]

The degree of safety within smart cities is important, but no city, even Singapore, can be completely protected all the time from every potential threat. For instance, in 2018 Singapore's online health network, "SingHealth," was successfully hacked resulting in the compromise of "1.5 million patient records," including the record of Singapore's Prime Minister Lee Hsien Loong.[213] The SingHealth investigation revealed that employees who

[208] The Economist Intelligence Unit, Safe Cities Index 2017 Security in a rapidly urbanizing world (Longdon, England: Economist Intelligence Unit, Ltd, 2017), https://dkf1ato8y5dsg.cloudfront.net/uploads/5/82/safe-cities-index-eng-web.pdf., 9, 17.

[209] Victor Loh, "The Big Read: As More Cyber Attacks Loom, Singapore Has a Weak 'First Line of Defence'," *TODAY*, October 26, 2019, https://www.todayonline.com/big-read/big-read-more-cyber-attacks-loom-singapore-weak-first-line-defence.

[210] Loh, "The Big Read: As More Cyber Attacks Loom, Singapore Has a Weak 'First Line of Defence.'"

[211] Seow Bei Yi, "Parliament: Strict Regime to Ensure Data Privacy in Police Camera Footage; 5,000 Cameras Already Installed," *The Straits Times*, February 6, 2018, https://www.straitstimes.com/politics/parliament-strict-regime-to-ensure-data-privacy-in-police-camera-footage-5000-cameras.

[212] Yi, "Parliament: Strict Regime to Ensure Data Privacy in Police Camera Footage; 5,000 Cameras Already Installed."

[213] Cyber Security Agency of Singapore, Singapore Cyber Landscape 2018 (Singapore: Cyber Security Agency of Singapore, 2019), http://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018., 3.

handled health records had a lack of understanding of what a cyber security incident was or what the reporting process was once a cyber-attack was discovered.[214] This theme is consistent with a Singapore online public awareness survey in 2019 that showed that Singaporeans were complacent with online activity and lacked concern for cyber threats.[215]

B. CASE STUDY: DENMARK

This portion of the chapter uses Denmark in comparison to the United States and Singapore to examine the similarities and differences of governmental priorities that influenced how they executed their smart city strategies. Denmark, the United States and Singapore have similar concerns regarding the impact that smart city strategies have on citizens' privacy and security. Denmark's geography, constitution and governmental construct and its historical path taken towards the adoption of a smart city strategy are different from the United States and Singapore. Denmark is considered a shining example to the world of how to execute a smart city strategy, making it an appealing case study. Denmark's membership within the European Union and its geography raises unique challenges in relation to urban communities' reliance on public services, energy, and the affects felt from climate change that the U.S. and Singapore may not relate to.

This segment of the chapter starts with a brief description of Denmark's geography, government makeup, key policy goals and main events that led to the origins of Denmark's adoption of a smart city plan. The development of smart infrastructure, public services, and personal data is discussed to provide context to how these elements are managed and regulated in a smart city framework. Consequently, privacy, security, and the separation of powers will be discussed to provide the social and governmental dynamics at play that effect how Denmark institutes its smart city plan and how it can be used in the United States to avoid the same challenges.

[214] Loh, "The Big Read: As More Cyber Attacks Loom, Singapore Has a Weak 'First Line of Defence.'"

[215] Loh, "The Big Read: As More Cyber Attacks Loom, Singapore Has a Weak 'First Line of Defence.'"

1. History and Origins of Denmark's Smart City Strategy

In contrast to the United States and Singapore, Denmark is geographically connected to Germany and at the same time possesses hundreds of archipelagic islands.[216] Mogens Rüdiger points out that the location of Denmark makes it a place for extremely cold winter seasons causing a significant dependency on energy imports from oil producing countries as a primary heating source.[217] Denmark has a population of over 5 million people, with the majority of its populace who are older and ailing, placing increased pressure on its healthcare system.[218]

In 1849, the organization of Denmark's government was established; transitioning its political system from an absolute monarchy into a constitutional monarchy responsible for representing the millions of Danish citizens.[219]

Denmark has been a part of many conflicts throughout the history of Europe. However, none have been as impactful on its future security and well-being of its people as the 1973 Yom Kippur War.[220] Denmark suffered from actions taken by the Organization of Arab Petroleum Exporting Countries (OAPEC) in response to the Yom Kippur War between Israel and Arab States (Egypt and Syria) by instituting an oil embargo against Israel and their western country supporters.[221] At the time, Denmark was overly dependent on oil imports from oil-producing countries for the heating of homes and transportation.[222]

Prior to the crisis, Denmark had not played a key role or established relevant policies in how the energy sector functioned.[223] Denmark's Prime Minister Anker

[216] "Denmark – Country Profile," nationsonline.org, 2019, http://www.nationsonline.org/oneworld/denmark.htm.

[217] Mogens Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," *Historical Social Research Historische Sozialforschung.* 39, no. 4 (January, 2014): 94,112, http://doi.org/10.12759/hsr.39.2014.4.94-112.

[218] nationsonline.org, "Denmark – Country Profile."

[219] nationsonline.org, "Denmark – Country Profile."

[220] Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," 19.

[221] Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," 100.

[222] Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," 101.

[223] Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," 110.

Jorgensen and the Danish Parliament kick-started a structural shift in their country's reliance on oil.[224] It responded with a national energy policy and regulatory structure that encompassed key initiatives predicated on the restriction of complacent behavior towards the usage of energy and drive for energy savings.[225]

Over time, Denmark's energy policies have evolved with the rise of technology's role in urban development and city management. During the 1970s, Denmark's environmentally sustainable development policies were focused on "end-of-pipe"[226] and pollution issues dealing with wastewater, transportation, and energy triggered by the aforementioned oil crisis.[227] As the usage of technology in cities had increased, Denmark turned its attention to "clean technologies and product design approaches between the 1980s and 1990s."[228] More recently in 2010, when the Smart City concept was introduced in Denmark, they shifted their attention towards a Sustainable Smart City Strategy.[229] The purpose of the strategy was to answer the challenges within its urban communities in "the use of data, sensors, and autonomous machines and vehicles" with a "human-centric governance framework."[230] Not only is technology helping optimize Denmark's public infrastructure, services, and limited resources but technology is increasing its role in the operation and security of Denmark's cities.

2. Denmark Smart Infrastructure and Public Service Delivery

For Denmark's sustainable smart city strategy to be effective, it needed a robust smart infrastructure capable of driving down pollution, increasing energy efficiency, and

[224] Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," 99, 101.

[225] Rüdiger, "The 1973 Oil Crisis and the Designing of a Danish Energy Policy," 99, 101.

[226] "Denmark - National Policies for sustainable development," The SusNordic Gateway, October 20, 2008, http://folk.uio.no/kristori/prosus/susnordic/denmark/national_policies/index.html.

[227] The SusNordic Gateway, "Denmark – National Policies for sustainable development."

[228] The SusNordic Gateway, "Denmark – National Policies for sustainable development."

[229] State of Green, "*Smart Cities - Creating liveable, sustainable and prosperous societies*," Version 1.0 (Denmark: State of Green, 2018), https://stateofgreen.com/en/uploads/2018/05/Smart-Grid.pdf?time=1546533259, 6.

[230] State of Green, "Smart Cities – Creating liveable, sustainable and prosperous societies," 6.

delivering public services to its citizens. Similar to Singapore, Denmark understood that the construction of a smart infrastructure depended on the coordination between public-private stakeholders working together to find ways for a municipal approach for governance, funding, and operations across multiple public domains.[231]

For these reasons, in 2013, Denmark formed the "Danish Smart City Network"[232] in support of implementing its Smart City strategy.[233] Denmark's coordination efforts were effective in creating a smart infrastructure which consisted of a Danish Basic Data platform interconnected with information-communications technology combined with an advanced energy smart grid.[234] According to the 2018 Global Connectivity Index, Denmark ranked 7th for its overall digital infrastructure and its contribution towards the transformation of industry, cities, and government.[235]

The changes in the lives of Danish citizens have accelerated due to the increased availability and access to online public services provided by its digital infrastructure. Like Singapore, Denmark's smart infrastructure platform became the major conduit for delivering public services to citizens in Denmark. Denmark uses its smart infrastructure to serve the public through the internet domain in the following areas: utilities, transportation, healthcare, legal, finances, education and other services.[236] Public services are integral to

[231] The Ministry of Foreign Affairs of Denmark, *Growing Smartcities In denmark* (Denmark: Arup, CEDI, 2016), http://um.dk/da/nyheder-fra udenrigsministeriet/newsdisplaypage/~/media/UM/Markedsinformation%20Publications/Growing_Smart_Cities_in_Denmark.pdf., 12.

[232] "Smart City Network," Smart Aarhus, 2015, https://www.smartaarhus.eu/projects/smart-city-network.

[233] Smart Aarhus "Smart City Network,"

[234] State of Green, "Smart Cities – Creating liveable, sustainable and prosperous societies," 9.

[235] Huawei Technologies Co., Ltd*, Global Connectivity Index 2018, Tap Into New Growth With Intelligent Connectivity* (Huawei Technologies Co., Ltd, 2018), https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180914., 7.

[236] Agency for Digitisation, Ministry of Finance, Denmark, *Wave 4 on Mandatory Self-Service* (Denmark: Ministry of Finance, 2015), https://en.digst.dk/policy-and-strategy/mandatory-digitisation/self-service/wave-4-on-mandatory-self-service/.

the society of Denmark because of the country's reputation as a welfare state based in part on the premise that its citizens should have the right to healthcare and education.[237]

Online public services are also important because Denmark has slowly converted to a "mandatory digital self-service and communications" program with the goal of adequately managing an ageing and ailing society.[238] For example; Denmark's "eHealth" platform allows communications between citizens, healthcare professionals and related systems.[239] Citizens can receive health consultations, prescriptions, personal health information and records via its eHealth platform.[240]

The same health information and records are stored in an eHealth database which can be accessed and shared between doctors, pharmacies, laboratories, and hospitals.[241] According to the 2018 Euro Health Consumer Index, Denmark's "Danish Digital Health Strategy" [242] is attributed with the country being ranked fourth for the utilization of its smart infrastructure in the delivery of health services to its citizens.[243]

The access to online public services has impacted the well-being of Danish citizens. According to the 2019 World Happiness Report, Denmark ranked second reflecting the Danish citizens' level of well-being in terms of satisfaction towards its government, "prosocial behavior,"[244] and digital technology's impact on society with regards to social media, personal data, and how they identify with their communities.[245]

[237] "Denmark - a Model Welfare Society," Copenhagen Capacity, accessed July 13, 2019, http://www.copcap.com/living-and-working/a-welfare-society.

[238] Agency for Digitisation, Ministry of Finance, Denmark, *Wave 4 on Mandatory Self-Service.*

[239] Patrick Kierkegaard, "EHealth in Denmark: A Case Study," *Journal of Medical Systems* 37 (December, 2013): https://doi.org/10.1007/s10916-013-9991-y., 2.

[240] Kierkegaard, "EHealth in Denmark: A Case Study," 2.

[241] Kierkegaard, "EHealth in Denmark: A Case Study," 2.

[242] Kierkegaard, "EHealth in Denmark: A Case Study," 2.

[243] Arne Bjornberg and Ann Y. Phang, *Euro Health Consumer Index 2018* (France: Health Consumer Powerhouse, 2019), https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf., 10.

[244] John F. Helliwell, Richard Layard and Jeffrey D. Sachs, *World Happiness Report 2019* (New York: The Sustainable Development solutions Network (SDSN), 2019, https://s3.amazonaws.com/happiness-report/2019/WHR19.pdf., 7.

[245] Helliwell, Layard and Sachs, *World Happiness Report 2019*, 28.

3. Privacy and Checks and Balances in Denmark

The increased usage of online public services by Danish citizens has resulted in the massive buildup of personal data that must be protected with technical mechanisms applied by organizations in control of personal data.

Denmark has enacted a set of personal data laws to ensure personal information is protected from improper usage. Namely, Denmark passed the Danish Data Protection Act of 2018 and has adopted the European Union's General Data Protection Regulation of 2016.[246] Denmark's "Datatilsynet" (Data Protection Agency) and the European Data Protection Board enforce personal data protection laws by regulating how domestic and international organizations handle physical and online personal information.[247]

At the same time, recent personal data breaches in Denmark leave many Danes skeptical of the effectiveness of the Danish Data Protection Agency and policies. For instance, it was reported in 2018 that over 40,000 Danish Facebook users had their personal information forwarded without consent to Cambridge Analytica for political use in Britain's Brexit bill and the 2016 U.S. election.[248]

In 2017, another controversy adding to the skepticism of Denmark's personal data laws emerged when the Danish Ministry of Justice authorized the police to use its "nationwide automatic number plate recognition [camera] system (ANPR)"[249] for public surveillance. It used the system to scan and store the data of "up to 600,000 vehicle registration plates a day."[250] Furthermore, the authorization allowed the police to utilize a

[246] Bjornberg and Phang, Euro Health Consumer Index 2018, 2.

[247] DLA Piper, *Data Protection Laws of the World, Denmark vs United Kingdom* (United Kingdom, DLA Piper, 2017), https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=DK&country-2=GB, 3.

[248] Catherine Stupp, "Cambridge Analytica harvested 2.7 million Facebook users' data in the EU," *EURACTIV.COM. Ltd*, April 6, 2018, https://www.euractiv.com/section/data-protection/news/cambridge-analytica-harvested-2-7-million-facebook-users-data-in-the-eu/.

[249] "Denmark: Targeted ANPR Data Retention Turned into Mass Surveillance," *EDRi* (blog), September 6, 2017, https://edri.org/denmark-targeted-anpr-data-retention-turned-into-mass-surveillance/.

[250] Lucie Rychla, "Danish Police Allowed to Scan Thousands of Licence Plates," *Online Post,* January 12, 2016, http://cphpost.dk/news/danish-police-allowed-to-scan-thousands-of-licence-plates.html

Global Positioning System (GPS) with ANPR to help recreate the location and route of personal vehicles suspected of crimes.[251]

Personal data security and online privacy are not the same. Unlike personal data security, online privacy goes a step further legally in whether organizations are allowed to share personal information with others and how that information is interpreted to other parties.[252]

Privacy and trust between citizens and government affect how society functions. A constitution is a contract between citizens and politicians based on trust that the government will defend the people's rights akin in part to values like online privacy.

Like the United States, Denmark's constitution includes the right to privacy and has instituted various data-privacy laws for added protection.[253] Denmark has committed to the United Nation's "International Covenant on Civil and Political Rights (ICCPR),"[254] extending the protection of privacy to its citizens to places abroad.[255] This shows that the Danish government is committed to preserving privacy as a social value domestically and internationally.

Safeguarding and keeping online Personally Identifiable Information (PII) and communications private is known as "ePrivacy."[256] Denmark subscribes to the European

[251] Rychla, "Danish Police Allowed to Scan Thousands of Licence Plates."

[252] "Data Security vs. Data Privacy - Why It Matters," *Managed Solution* (blog), September 13, 2018, https://www.managedsolution.com/data-security-vs-data-privacy-why-it-matters/.

[253] Privacy International and IT-Political Association of Denmark, *The Right to Privacy in Denmark,* 24th Session (London: Privacyinternational.org, 2015), https://privacyinternational.org/sites/default/files/2017-12/Denmark_PI_UPR%20Stakeholder_submission_FINAL.pdf., bullet. 9, 10.

[254] Privacy International and IT-Political Association of Denmark, *The Right to Privacy in Denmark*, bullet 11.

[255] Privacy International and IT-Political Association of Denmark, *The Right to Privacy in Denmark*, bullet 10.

[256] Daniela Popescul and Laura D. Radu, "Data Security in Smart Cities: Challenges and Solutions," *Informatica Economica; Bucharest* 20, no. 1 (January, 2016): 29–38, http://dx.doi.org/10.12948/issn14531305/20.1.2016.03., 35.

Parliament's personal data directive (2016/680)[257] That states' controllers of personal data shall design and employ a privacy by default system capable of retaining only the amount of personal data necessary for a specific purpose.[258] This ensures that Danish organizations that manage personal information are in compliance with domestic and international personal data privacy laws while conducting business.

Despite that, Denmark exempts some of its general personal data protections for its Ministry of Defense and Intelligence agencies in the matters concerning foreigners and anti-terrorism operations.[259] The above-mentioned agencies are allowed to collect "raw data" domestically on Danish citizens and retain it for up to "15 years."[260] For instance, Danish domestic and European Union related airline companies share passenger, name, and record information with Denmark's law enforcement agencies in support of security operations.[261]

Denmark's system of checks and balances in relation to the balancing of its security measures with civil liberties rests with its constitution.[262] Denmark's intelligence and security oversight committees and justice department have the authority to call out excessive overreaches in Danish law enforcement operations concerning the surveillance and collection of its citizens' personal data.[263] However, Denmark's adjudication capacity

[257] European Parliament and of the Council, *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016*, Pub. L. No. 32016L0680 (Brussels: European Parliament and of the Council, 2016), http://data.europa.eu/eli/dir/2016/680/oj/eng., bullet 53.

[258] Popescul and Radu, "Data Security in Smart Cities," 34.

[259] Privacy International and IT-Political Association of Denmark, *The Right to Privacy in Denmark,* bullet 30, 36.

[260] Privacy International and IT-Political Association of Denmark, *The Right to Privacy in Denmark*, bullet 30.

[261] European Commission, "Passenger Name Record (PNR)," Migration and Home Affairs - European Commission, December 6, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.

[262] Danish Institute for Human Rights, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies* (Denmark: Danish Institute for Human Rights, 2014), http://edz.bib.uni-mannheim.de/daten/edz-b/ebr/14/FRA_2014_denmark_Vol%20I_Fundamental%20rights%20safeguards%20and%20remedies%20in%20the%20EU.pdf., 6.

[263] Danish Institute for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 6.

is limited to the associated law in question and is not able to litigate Denmark's executive office's "discretionary powers" in the application of Danish law.[264]

4. Security

Similar to the United States and Singapore, Denmark has created security policies and organizations in support of its smart city ecosystem to protect its public from domestic and international threats. Denmark's security measures of effectiveness depends on a variety of elements. In 2011, Denmark's Agency for Digitization was established under its Ministry of Finance with the purpose of administering digital city policies dealing with the operations, security, and online services provided to the public.[265]

The Danish Centre for Cyber Security (CfCS), the Danish Security and Intelligence Service (PET) and Danish Defense Intelligence Service (DDIS) agencies are the enforcement agencies for smart city security and policy in Denmark.[266] These agencies work together in preventing physical and cyber-crime and terrorism, domestically and abroad.[267]

The Danish Centre for Cyber Security (CfCS) is Denmark's agency for dealing with cyber threats to its information-communications infrastructure by using its civil and military Computer Emergency Response Teams (CERTs).[268] The agency has nearly unlimited authority stemming from its Centre for Cyber Security Act and from the exemptions the agency has from personal data laws to collect and monitor information that

[264] Danish Institute for Human Rights, National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies, 6.

[265] Agency for Digitisation, "About the Agency for Digitisation," Ministry of Finance – Denmark, July 15, 2019, https://admin.en.digst.dk/about-us/.

[266] Danish Institute for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 2–3.

[267] Danish Institute for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 3.

[268] Danish Institute for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 3.

passes over public-private digital networks “without [a] court order.”[269] The same information can be passed to other law enforcement agencies without consent for further investigation and even retained for up to “3 years” if needed.[270]

Denmark has security policies that cover the physical and cyber domains within their smart city framework.[271] However, its cyber security policies appear to be insufficient when compared to Singapore and the U.S. Denmark’s cyber security policies lack a critical infrastructure plan and lacks a public-private partnership agreement, and has no mandatory reporting requirement for “cybersecurity incidents” within the private sector domain.[272]

In 2018, Denmark’s “Cyber and Information Security Strategy” called attention to the rise of vulnerabilities in response to the growing digitization of Denmark cities.[273] According to the strategy, the pervasiveness of online networks and their interconnected complexities make cyberattacks more easily and cheaply obtainable.[274] What’s more, the Danish people’s overreliance and lack of “security culture” [275] amplify network vulnerabilities.[276]

Denmark has established initiatives for the mitigation of cyber vulnerabilities to its national security. Some of its key initiatives are causing shifts in Denmark’s national security landscape at the public and private echelons of its society. First, several national

[269] Danish Institute for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 3.

[270] Danish Institute for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 3.

[271] International Comparative Legal Guides (ICLG), *Compare & Research The Law. Worldwide* (London, United Kingdom: Global Legal Group, 2019), https://iclg.com/.

[272] BSA The Software Alliance, *EU Cybersecurity Dashboard A Path to a Secure European Cyberspace* (Washington, D.C.: Galexia, 2015), http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf., 8, 9.

[273] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy* (Greece: ENISA, 2018), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-strategy-for-cyber-and-information-security., 9.

[274] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy*, 9.

[275] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 9.

[276] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 9.

centers of security experts from public-private spheres are being organized to monitor and respond to threats to public online services, infrastructure, and data in real time.[277] Second, Denmark's government is educating and raising public awareness of cyber threats along with providing online portals for citizens to report online crime.[278]

Similarly, Denmark's government defines what the national technical and organizational[279] security requirements are and have mandated that public and private organizations fulfill them.[280] Unlike the United States or Singapore, Denmark puts more of the burden for investment and protection standards on the private sector, but provides security agencies as an emergency response resource for addressing potential threats. Denmark is unique from the United States in that it divides the onus for security investment and responsibility between public and private institutions with limited direct funding support.[281]

[277] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 17, 24, 35.

[278] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy* 27.

[279] "Security in Denmark – DLA Piper Global Data Protection Laws of the World," DLA Piper, January 10, 2019, https://www.dlapiperdataprotection.com/index.html?t=security&c=DK.

[280] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 9.

[281] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 9.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS

A comparative case study analysis provided in Chapter III between Singapore and Denmark found significant affects from smart city infrastructure's influence on the homeland security landscape and its impact on public services and security of citizens. There were correlations between the increased usage of smart city services and smart technologies and vulnerabilities within urban communities. Vulnerabilities will continue to grow as municipalities incorporate more technology in the linking of citizens to government services. The significance of security and privacy in Denmark's and Singapore's approaches to smart city implementation became apparent through the research and are outlined below.

The balance of security and privacy in smart communities depends on the degree of collaboration between public-private organizations responsible for smart city governance when it comes to design, strategy, policy, investment and education. Finding the right balance between security and privacy through effective collaboration in smart city design builds trust with online public users.

Singapore and Denmark started towards smart city design in their efforts for solving challenges related to rapid urbanization and limited resources that helped accelerate the need for the use of technology. Eventually each government discovered that it could not effectively implement a smart city design on their own because of the interests, issues, and skills needed from the private and academic communities. Public-private collaboration accelerated the innovation and development of the smart city concept used by each country.

Singapore and Denmark were effective in the implementation of their smart city strategies because of their respective governments initially led the collaboration efforts, then incrementally shifted part of the smart city developmental role to the private and educational sectors. This helped both countries save money by reducing redundant resources and increased overall standardization of technology-infrastructure used in their smart city designs. Both governments maintained control of the formulation of security directives that the public and private sector were mandated to follow.

Additionally, a unified effort and long-term outlook in Denmark's and Singapore's planning process facilitated more efficient procurement of materials, construction process, policy formulation and investment in smart city development.

Furthermore, effectiveness of the planning process for smart city design depends on the inclusion of public-private and key community stakeholders. Stakeholder inclusiveness is essential for encouraging the communication of vulnerabilities of smart city infrastructure and management details. It stimulates discussion about who is responsible for what types of support for security, safety, and management in the usage of smart city technology for the delivery of public services.

Increasing the access of smart city services to all sections of society promotes participation in the partaking of public services and helps improve city governance within urban communities. Inclusion helps affected citizens by increasing their public awareness, education, and promotes the well-being of smart city inhabitants, especially the poor.

A. PRIVACY

The U.S., Singapore, and Denmark perceive the issue of privacy differently from a societal and legal standpoint. Unlike Singapore and Denmark, the right to privacy in the U.S. is embedded in the constitution, creating a legal and social contract that obligates the U.S. government in providing adequate protection for personal privacy rights.

However, the protection of privacy is much more difficult when the complexities of technology are involved. Many public-private services provided in a smart environment have loopholes when it comes to privacy. Part of the reason is due to the rapid rollout of security parameters after major incidents happen without fully considering the design features and policies needed for assuring privacy of smart communities. Another reason is because privacy takes a backseat when governments levy exemptions for the sake of fighting terrorism and crime.

Another way of looking at privacy concerns in the implementation of smart cities is that there are cultural and political differences between countries that affect the way privacy is regarded. Some cultures in places like Singapore appear not to value personal privacy the way America does. The Singapore culture in some cases value the common good and security of the population more than privacy. Perhaps this can be attributed to the traditionally embedded values of discipline and order found within its Confucian culture. Singapore's politics reflect this attitude in the way it prioritizes security policies and regulations over privacy protections. This could explain why the Singapore government has been able to manage and suppress public dissent over privacy issues by employing aggressive surveillance, monitoring, and usage of personal user data.

B. SECURITY

The main theme tied to security in smart cities that has emerged deals with cyber threats to related networks, online public service platforms, the mishandling of personal data, and insufficient training for public service workers. These security-associated threats include internal and external state and non-state actors.

Countries like Singapore and Denmark are deploying smart city technology to help in reducing crime while improving the overall well-being of their populations. Effective national security transformations in response to an emerging high-tech world in the comparative case study analysis of Denmark and Singapore tend to incorporate policies and measures that emphasizes public access, awareness, education and consumer rights. For example, as described in Chapter III, Denmark implements preventative security measures to mitigate abusive usage and access of smart city networks. The preventative security measures include a national unique online identification program comparable to a digital lock and key model that appreciably improves the protection of its online public service forums.

Another smart city security measure used by Denmark's government is the Cyber Emergency Response Teams (CERTs) Agency concept. The concept consists of teams that are made up of cyber-defense, emergency responders, and law enforcement security professionals from national, state, and local agencies capable of coordinating and responding to threats to government-run information technology platforms. Denmark's CERTs agency concept has helped by decreasing the damages from cyberattacks on Denmark's smart network users.

From a law enforcement perspective, the growing usage of surveillance cameras and sensors within smart cities helps reduce physical and cybercrime. The ability for law enforcement officials at the city level to use cyber, sensors and data on a 24-hour basis in monitoring smart populated areas helps improve a real time response to emergency situations. Additionally, it helps connect emergency responders to law enforcement, security and other agencies to help manage the welfare of citizens and assist affected populations under duress.

V. CONCLUSION AND RECOMMENDATIONS

This research sought answers to problems originating in the convergence of smart city development and online public service forums with a newly encompassing homeland security composition. Overall the qualitative case study examination of smart city strategies implemented in Singapore and Denmark concludes that smart technology implementation creates both new opportunities and problems for urban communities as noted in Chapter I. The reasoning behind smart city implementation is to improve the well-being of smart urban societies. A shared smart city network that serves the public can help save time, money, and resources. Smart city networks can help governments capitalize on the usage of personal data to help fulfill various human aspects and interests of diverse populations in an increasingly globalized world. Nonetheless, this research highlights the inadequacies of smart city design and related operational conventions and raises awareness about the introduction of physical, cyber, and organizational weaknesses left to be exploited in a smart city environment.

Chapter II centered on major challenges hindering adequate non-invasive security measures in promoting the maximization of benefits that smart cities intend to provide. Online personal data is generated at an ever-growing scale that is transforming into big data as a consequence of growing human reliance and interactions with online public services. Personal data can divulge the identity, behavior, and intent of people’s actions. Such information should be shared between federal, state, private, and local law agencies involving national security and to prevent greater negative impacts to smart societies as a whole. But the security sharing aspect is only half of the equation that requires a counterbalancing action of privacy protection in support of the individual. Additionally, smart city standardization emerged as a structurally significant underpinning component necessary for facilitating the management of big data, sharing of information, privacy protection, and for reducing the cumulation of societal risk.

Chapter III presented a case study comparison between Singapore and Denmark in the origins and implementation of smart city strategies. The case study analysis showed unique characteristics behind each country’s methods and approaches used in public services delivery and security for the overall well-being of society. Each case study demonstrated that smart city planning, policy, interagency coordination, and standardization are significant tools that can be leveraged to lessen the risk of unauthorized privacy intrusions on citizens while maintaining an effective level of security.

Chapter IV provided insights that revealed that countries, like the U.S., that are working towards smart city development planning are more effective when the process is government led, public-private stakeholders are involved, and when there is a long-term outlook for implementation. Security and privacy are vital aspects that must be addressed during the planning process. Security measures must deal with both intentional and unintentional misuses of smart city generated data and technology. Privacy issues in smart urban communities emerge because privacy is usually an afterthought in smart city development as smart city planners and governments rush the integration of technology into cities. Hasty smart city implementation causes governments to be reactive when it comes to fixing privacy-related smart city policies and security applications related to information sharing. Governments can help alleviate these security and privacy problems by controlling network access and raising public awareness about good practices that citizens should use in smart city interactions.

A. RECOMMENDATIONS

The U.S. and other country's taking part in smart city concept implementation have made adjustments to policy, planning, and development in an effort to tackle security and privacy challenges stemming from online public service delivery. However, this research discovered problems with smart city strategy formulation, coordination, privacy and security. These problems can be resolved with my following recommendations related to collaboration, security, and privacy to help improve smart city policy, strategy, and execution.

1. Collaboration

As stated in Chapter IV, the level of public-private collaboration is the key to finding the right balance between privacy and security in a smart city strategy.

Collaboration in smart city implementation can be improved through a top-down smart city organizational command and control structure.

The organizational structure should consist of four echelons. The echelons should consist of a congressional oversight committee, U.S. national, regional, and urban smart city offices and include the following:

Congressional smart city oversight committee made up of leaders in congress. They would review and implement policy recommendations from smart city stakeholders and lower organizational echelons about related management problems and solutions that should be addressed.

U.S. national smart city office that includes experts from Department of Homeland Security (DHS), Department of Energy (DOE), American Civil Liberties Union (ACLU), U.S. Office of Science and Technology (OST), smart city projects representatives (mixture between academia and private industry representatives).

U.S. regional smart city offices (i.e., West, East, North, South) that include professionals from the Department of Homeland Security (DHS), intelligence-fusion centers, State law enforcement, American Civil Liberties Union (ACLU), Department of Energy (DOE) and smart city project representatives.

U.S. urban smart city offices should be added within participating smart city communities. Urban smart city offices should include the involvement of the mayor, emergency services, law enforcement, local public utilities (energy and communications), private industry leaders, and community organizers.

Each echelon should hold meetings and hearings periodically to address the related condition, implementation, lessons learned, and concerns that emerge from smart city implementation. The smart city organization structure should be flexible in authority and in decision making processes. The organizational structure should be decentralized in decision making when it comes to responding to related smart city physical and cyber emergencies. The smart city organizational structure would be more centralized in decision making in terms of planning, policy formulation, design and implementation. Additionally, expert involvement and collaboration at all organizational echelons for smart city governance brings valuable insights to smart city infrastructure, security and privacy in the online public services used by smart urban populations.

2. Security

From a security standpoint, I recommend the U.S. use a two-pronged approach. First, the U.S. should use Denmark's model described in Chapter III and IV for responding to cyber threats in the form of a Cyber Emergency Response Team (CERT) agency concept be replicated and modified slightly. The U.S. should expand the CERT model with an added physical security component, resulting in a U.S. Physical-Cyber Emergency Response Team (P-CERT).

This security component should be implemented at the U.S. regional and local urban smart city organizational echelons. P-CERT professionals would be provided initial and follow-on periodic training. They would work together with regional Department of Homeland Security (DHS) fusion centers by employing intelligence gathered under reasonable suspicion to help thwart physical or cyber threats within smart cities.

This security approach can help improve real-time responses to criminal, emergency, and terrorist type activity within smart cities. Moreover, it bridges the security gap between the cyber and physical domains where the eventuality of automated technology is expected to operate and manage public services, infrastructure, human, and machine interactions with smart city functions.

Additionally, the U.S should replicate Denmark's digital identification initiative. The security initiative is a government "Easy ID"[282] program that enables its citizens to use a national digital signature to access online public services globally and through a government portal that spans across multiple agencies.[283]

[282] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 25.

[283] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 32.

3. Privacy

I recommend the following for the privacy of smart city citizens. First, the U.S. government should provide and control a main smart city network (physical and cyber) in cities that desire to adopt a smart city concept.

The smart city network should only be accessed by people with a nationally approved form of digital identification.[284] A government-provided online public service portal would allow security agencies to monitor online activity occurring within the portal.

Public-private organizations that desire to offer public services to citizens must utilize the portal. These organizations would be responsible for safeguarding private personal information generated through public service interactions. However, they would also be responsible for utilizing government-approved security software, programs, and hardware that help them detect cyber or physical violations. It would also be mandatory for these companies to report such violations to their customers and to local and regional Physical-Cyber Emergency Response Team (P-CERT) representatives.

Additionally, the meaning of personal privacy is changing in response to smart city developments taking place around the world. There are limitations to the protection of personal privacy when it comes to government-provided services or infrastructure. U.S. Security and law enforcement agencies can legally conduct reasonable searches if they suspect criminal or threatening activities that may occur within smart city physical and cyber domains.

As for smart city societies, the American Civil Liberties Union (ACLU), community organizers, city councils, and city residents must be involved with the planning, implementation, and ongoing usage of smart city technologies. For instance, the ACLU has found a way to protect smart city residents by collaborating with local city governments and law enforcement agencies through the establishment of Community Control Over

[284] The European Union Agency for Cybersecurity, *Danish National Cyber Security Strategy,* 25.

Police Surveillance (CCOPS) laws in 2016.[285] The CCOPS approach helps residents in working with their respective city councils "to decide if and how surveillance technologies are used, through a process that maximizes the public's influence over those decisions."[286] Furthermore, CCOPS "include a transparent approval process that requires public disclosure, open hearings, and sign-off from elected officials on all surveillance technologies and the specific ways in which they intend to use them."[287]

4. Further Research

Future research should evaluate how big data management will impact the effectiveness of smart city operations, privacy and security measures used in the governance of smart communities as the technology continues to progress and becomes more pervasive.

Further study should also look at how culture, trust, and the behavior of a society affects populations that have inhabited smart city communities for longer than ten or more years. A cultural study that involves the habits of smart communities may help smart city planners understand the differences in terms of acceptability of security and privacy standards among society. Understanding such differences may help planners more accurately insert more effective security and privacy policies in their approaches to the formulation of smart city strategies.

[285] "Community Control Over Police Surveillance," American Civil Liberties Union, May 3, 2019, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

[286] American Civil Liberties Union, "Community Control Over Police Surveillance."

[287] Marlow and Saifuddin, "How to Stop 'Smart Cities' From Becoming 'Surveillance Cities.'"

LIST OF REFERENCES

Acemoglu, Daron, James A Robinson, and Ragnar Torvik. "Why Do Voters Dismantle Checks and Balances?" Working paper, National Bureau of Economic Research. https://www.nber.org/papers/w17293.pdf.

Agency for Digitisation, Ministry of Finance, Denmark. *Wave 4 on Mandatory Self-Service.* Denmark: Ministry of Finance, 2015. https://en.digst.dk/policy-and-strategy/mandatory-digitisation/self-service/wave-4-on-mandatory-self-service/.

Agency for Digitisation. "About the Agency for Digitisation." Ministry of Finance - Denmark. July 15, 2019. https://admin.en.digst.dk/about-us/.

Albert, Richard. "The Separation of Higher Powers." *SMU LAW REVIEW* 65, no. 1 (July 2012): 3–69. https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1407&context=lsfp.

Athey, Susan, Christian Catalini, and Catherine Tucker. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." Working Paper, National Bureau of Economic Research, 2017. https://www.nber.org/papers/w23488.pdf.

Avenue, Human Rights Watch | 350 Fifth, 34th Floor | New York, and NY 10118-3299 USA | t 1.212.290.4700. "Singapore: Space Narrows for Online News Media." Human Rights Watch, October 15, 2014. https://www.hrw.org/news/2014/10/15/singapore-space-narrows-online-news-media.

Bailey, Tom. "How Singapore Married Dictatorship with a Market Economy." *World Finance The Voice Of The Market*. July 16, 2015. https://www.worldfinance.com/special-reports/how-singapore-married-dictatorship-with-a-market-economy.

Bélanger, France, and Robert E. Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35, no. 4 (December 2011): 1017–41. https://doi.org/10.2307/41409971.

Bjornberg, Arne and Ann Y. Phang. *Euro Health Consumer Index 2018.* France: Health Consumer Powerhouse, 2019. https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf.

BSA The Software Alliance. EU Cybersecurity Dashboard A Path to a Secure European Cyberspace. Washington, D.C.: Galexia, 2015. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

Busch, Lawrence. *Standards : Recipes for Reality*. Infrastructures Series. Cambridge, Massachusetts: MIT Press, 2011. ProQuest.

CACM Staff. "Big Data." *Communications of the ACM* 60, no. 6 (June 2017): 24–25. https://doi.org/10.1145/3079064.

Clark, Greg, and Tim Moonen. *World Cities and Nation States*. Chicester, UNITED KINGDOM: John Wiley & Sons, Incorporated, 2017. ProQuest.

"Community Control Over Police Surveillance." American Civil Liberties Union. Accessed May 3, 2019. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

Copenhagen Capacity. "Denmark - a Model Welfare Society." Accessed July 13, 2019. http://www.copcap.com/living-and-working/a-welfare-society.

Cornell University, INSEAD, and the World Intellectual Property Organization. *Global Innovation Index 2018: Energizing the World with Innovation.* Geneva, Switzerland, by the World Intellectual Property Organization (WIPO), and in New Delhi, India, and by the Confederation of Indian Industry: Ithaca, Fontainebleau, and Geneva, 2018. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018.pdf.

Cyber Security Agency of Singapore. *Singapore Cyber Landscape 2018*. Singapore: Cyber Security Agency of Singapore, 2019. http://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018. http://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018.

"Csasingaporecyberlandscape2018.Pdf." Accessed July 13, 2019. https://www.csa.gov.sg/~/media/csa/documents/publications/csasingaporecyberlandscape2018.pdf.

———. Accessed July 15, 2019. https://www.csa.gov.sg/~/media/csa/documents/publications/csasingaporecyberlandscape2018.pdf.

"Cyber Crime Costs Projected To Reach $2 Trillion by 2019." Accessed July 13, 2019. https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6eb950993a91.

Danish Institute for Human Rights. *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies.* Denmark: Danish Institute for Human Rights, 2014. http://edz.bib.uni-mannheim.de/daten/edz-b/ebr/14/FRA_2014_denmark_Vol%20I_Fundamental%20rights%20safeguards%20and%20remedies%20in%20the%20EU.pdf.

Davenport, Thomas H. and Randy Bean, "Big Data and AI Executive Survey 2019." New Vantage Partners, January 2019. https://newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf.

DLA Piper. *Data Protection Laws of the World, Denmark vs United Kingdom.* United Kingdom, DLA Piper, 2017. https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=DK&country-2=GB.

———, "Security in Denmark - DLA Piper Global Data Protection Laws of the World." January 10, 2019. https://www.dlapiperdataprotection.com/index.html?t=security&c=DK.

Eggers, William, and John Skowron. "Smart City Overview | Deloitte Insights." Forces of Change: Smart Cities, March 22, 2018. https://www2.deloitte.com/insights/us/en/focus/smart-city/overview.html.

EDRi (blog). "Denmark: Targeted ANPR Data Retention Turned into Mass Surveillance." September 6, 2017. https://edri.org/denmark-targeted-anpr-data-retention-turned-into-mass-surveillance/.

The Economist Intelligence Unit. *SAFE CITIES INDEX 2017 Security in a rapidly urbanizing world.* London, England: Economist Intelligence Unit, Ltd, 2017. https://dkf1ato8y5dsg.cloudfront.net/uploads/5/82/safe-cities-index-eng-web.pdf.

European Commission. "Passenger Name Record (PNR)." Migration and Home Affairs - European Commission. December 6, 2016. https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.

European Parliament and of the Council. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016*. Pub. L. No. 32016L0680. Brussels: European Parliament and of the Council, 2016. http://data.europa.eu/eli/dir/2016/680/oj/eng.

The European Union Agency for Cybersecurity. *Danish National Cyber Security Strategy.* Greece: ENISA, 2018. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-strategy-for-cyber-and-information-security.

OECD. *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*. Paris: OECD iLibrary, 2013. https://read.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en#page1.

Freedomhouse.org. *Freedom On The Net 2015 Singapore*. Singapore: Washington, D.C.: Freedomhouse.org, 2015. https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Singapore.pdf.

———. *Singapore Partly Free*. Washington, D.C.: Freedomhouse.org, 2018. https://freedomhouse.org/report/freedom-net/2018/singapore.

The Constitution Project. *Recommendations for Fusion Center preserving privacy & civil liberties while protecting against crime & terrorism.* Washington, D.C.: The Constitution Project, 2012. https://constitutionproject.org/pdf/fusioncenterreport.pdf

Government Technology Agency (GOVTECH SINGAPORE). "MEDIA FACTSHEET National Digital Identity," 2018. https://www.smartnation.sg/docs/default-source/cos2018/national-digital-identity-factsheet.pdf.

Hage, Eveline, John P Roo, Marjolein AG van Offenbeek, and Albert Boonstra. "Implementation Factors and Their Effect on E-Health Service Adoption in Rural Communities: A Systematic Literature Review." *BMC Health Services Research* 13, no. 1 (December 2013): 19. https://doi.org/10.1186/1472-6963-13-19.

Hasbini, Mohamad, James Mckinlay, Martin Tom-pertersen, Aseem Jakhar, and Amgad Magdy. *Smart cities appeal and 15 things that should not go wrong*. N.p.: Securingsmartcities.org, 2017. https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-15-things-v1.3.pdf.

He, Meilin, Laura Devine, and Jun Zhuang. "Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach." *Risk Analysis* 38, no. 2 (August 2017): 215–25. https://doi.org/10.1111/risa.12878.

Helliwell, John F., Richard Layard and Jeffrey D. Sachs. *World Happiness Report 2019.* New York: The Sustainable Development solutions Network (SDSN), 2019. https://s3.amazonaws.com/happiness-report/2019/WHR19.pdf.

Hellström, Lina, Karolina Waern, Emelie Montelius, Bengt Åstrand, Tony Rydberg, and Göran Petersson. "Physicians' Attitudes towards EPrescribing – Evaluation of a Swedish Full-Scale Implementation." *BMC Medical Informatics and Decision Making* 9, no. 1 (December 2009): 37. https://doi.org/10.1186/1472-6947-9-37.

Higgins, Kelley J. "Spike In Power Grid Attacks Likely In Next 12 Months." Informa PLC Informa UK Limited. February 19, 2010. https://www.darkreading.com/vulnerabilities---threats/spike-in-power-grid-attacks-likely-in-next-12-months/d/d-id/1132982.

Holder, Sarah. "The Shadowy Side of LED Streetlights." CityLab. Accessed May 3, 2019. https://www.citylab.com/equity/2018/03/their-lights-were-watching-odd/554696/.

Huawei Technologies Co., Ltd. *Global Connectivity Index 2018, Tap Into New Growth With Intelligent Connectivity*. Huawei Technologies Co., Ltd, 2018. https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180914.

"Human Development Index (HDI) | Human Development Reports." Accessed July 11, 2019. http://hdr.undp.org/en/content/human-development-index-hdi.

———. Accessed July 12, 2019. http://hdr.undp.org/en/content/human-development-index-hdi.

International Comparative Legal Guides (ICLG). *Singapore: Data Protection 2019.* London, United Kingdom: Global Legal Group, 2019. https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore.

———. *Compare & Research The Law. Worldwide.* London, United Kingdom: Global Legal Group, 2019. https://iclg.com/.

"ISE-Impplan-200611.Pdf." Accessed May 3, 2019. https://permanent.access.gpo.gov/lps89195/ISE-impplan-200611.pdf.

Judicial Checks and Balances. Cambridge, Mass: National Bureau of Economic Research, 2003.

Kale, Vivek. *Creating Smart Enterprises*, n.d. https://www.taylorfrancis.com/books/9781315152455.

Kang, Alex. "FCC Privacy Rule Repealed." The Regulatory Review. April 6, 2017. https://www.theregreview.org/2017/04/06/kang-fcc-privacy-rule-repealed/.

Kegley and Blanton. *World Politics: Trend and Transformation*. 13th ed., 70..

Kenton, Will. "Unicameral System." Investopedia. Accessed July 15, 2019. https://www.investopedia.com/terms/u/unicameral-system.asp.

Kesler, Reinhold, Micheal E. Kummer, and Patrick Schulte, "Mobile Applications and Access to Private Data: The Supply Side of the Android Ecosystem." Working paper, Centre for European Economic Research, 2017. https://dx.doi.org/10.2139/ssrn.3106571.

Kierkegaard, Patrick. "EHealth in Denmark: A Case Study." *Journal of Medical Systems* 37 (December 1, 2013): 1–10. https://doi.org/10.1007/s10916-013-9991-y.

Kim, Won, Jeong, and Kim. "*A Holistic View of Big Data"* In *Big Data: Concepts, Methodologies, Tools, and Applications,* ed. Information Resources Management Association, 73–84. Hershey, Pennsylvania: Information Science Reference, 2016.

Koh, Thiam Seng, Sai Choo Lee, and Soh Tin Ho. *Information Communication Technology in Education: Singapore's ICT Masterplans, 1997–2008*. Singapore: World Scientific Publishing Co Pte Ltd, 2008. ProQuest.

KPMG. *Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line*. Report No. 134122-G. Switzerland: KMPG International, 2016. https://assets.kpmg/content/dam/kpmg/se/pdf/advisory/2016/se-Creepy-or-cool-report_web.pdf.

Kurlantzick, Joshua, "How Singapore's People's Action Party Continued Its 50-Year Reign." *The National*, September 24, 2015. https://www.thenational.ae/arts-culture/how-singapore-s-people-s-action-party-continued-its-50-year-reign-1.126824.

Kurtz, Jennifer A., Roland J. Cole, and Isabel A. Cole. *Politics, Democracy, and e-Government Participation and Service Delivery*. Hershey, Pa.: Information Science Reference, 2010. https://doi.org/10.4018/978-1-61520-933-0.

Laney, Doug. "3D Data Management Controlling Data Volume Velocity and Variety." *Gartner* (blog), February 6, 2001. https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Langenberg, Tobias. *Standardization and Expectations.* Berlin, Heidelberg: Springer, 2006. https://doi-org.libproxy.nps.edu/10.1007/3-540-28113-4.

Lee, Terrence. "Singapore an Advanced Surveillance State, but Citizens Don't Mind." *Tech in Asia*, November 25, 2013. https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind.

Lee, Kevin T. Y. "The Evolution Of Singapore's Modern Constitution: Developments From 1945 To The Present Day." *Singapore Academy of Law Journal* 1 (1989): https://ssrn.com/abstract=626724

Liu, and Shuhua Yuan Qianli Monica. "Urban Community Grids Management in Metropolitan China: A Case Study on Factors Contributing to Mobile Governance Success," 2013, 145–75.

Loh, Victor. "The Big Read: As More Cyber Attacks Loom, Singapore Has a Weak 'First Line of Defence,'" *Today*, October 26, 2019. https://www.todayonline.com/big-read/big-read-more-cyber-attacks-loom-singapore-weak-first-line-defence.

Lowman, Marie. *A Practical Guide to Analytics for Governments : Using Big Data for Good*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2017. ProQuest.

Managed Solution. "Data Security vs. Data Privacy - Why It Matters." September 13, 2018. https://www.managedsolution.com/data-security-vs-data-privacy-why-it-matters/.

Marlow, Chad and Maryiam Saifuddin, “How to Stop ‘Smart Cities’ From Becoming ‘Surveillance Cities.’” American Civil Liberties. September 17, 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-stop-smart-cities-becoming-surveillance-cities.

Marburger, John H, E. F Kvamme, George Scalise, and Daniel A Reed. “Leadership Under Challenge: Information Technology R&D in a Competitive World. An Assessment of the Federal Networking and Information Technology R&D Program,” 2007.

Marr, Bernard. *Big Data Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance*. West Sussex, United Kingdom: John Wiley & Sons, Incorporated, 2015. ProQuest.

McNamara, Thomas E. (Thomas Edmund). *Information Sharing Environment Implementation Plan*. ISE Implementation Plan. Washington, D.C.: Office of the Director of National Intelligence, Program Manager, Information Sharing Environment, 2006.

Meijer, Albert. “Datapolis: A Public Governance Perspective on ‘Smart Cities.’” *Perspectives on Public Management and Governance* 1, no. 3 (August, 2018): 195–206. https://doi.org/10.1093/ppmgov/gvx017.

Mesch, Gustavo S. “Ethnic Origin and Access to Electronic Health Services.” *Health Informatics Journal* 22, no. 4 (December 2016): 791–803. https://doi.org/10.1177/1460458215590863.

Miller, Fred. “Aristotle’s Political Theory in The Stanford Encyclopedia of Philosophy.” Metaphysics Research Lab, Stanford University. November 7, 2017. https://plato.stanford.edu/archives/win2017/entries/aristotle-politics/.

Mill City Press, Inc., “America’s Survival Guide.”

The Ministry of Foreign Affairs of Denmark. *Growing Smartcities In Denmark.* Denmark: Arup, CEDI, 2016. http://um.dk/da/nyheder-fra udenrigsministeriet/newsdisplaypage/~/media/UM/Markedsinformation%20Publications/Growing_Smart_Cities_in_Denmark.pdf.

Morabito, Vincenzo. *Big Data and Analytics Strategic and Organizational Impacts*. Cham: Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-10665-6.

Nationsonline.org, klaus kästle-. “Denmark - Country Profile - Nations Online Project.” Accessed July 13, 2019. http://www.nationsonline.org/oneworld/denmark.htm.

Nationsonline.org, “History of Singapore - Nations Online Project.” 2019. https://www.nationsonline.org/oneworld/History/Singapore-history.htm.

National Science and Technology Council. *National Privacy Research Strategy*. Washington, DC: Whitehouse, 2016. https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf

Nguyen, Tho H. *Leaders and Innovators : How Data-Driven Organizations Are Winning with Analytics*. Wiley and Sas Business Series. Hoboken: Wiley, 2016. ProQuest.

Obi, Toshio. *A Decade of World E-Government Rankings*. Global E-Governance Series ; Volume 7. Amsterdam: IOS Press, 2015.

Park, Patrick H. *Big Data War : How to Survive Global Big Data Competition*. First edition. Big Data and Business Analytics Collection. New York, NY 10017: Business Expert Press, 2016. ProQuest.

Petersen, Karen Lund, and Vibeke Schou Tjalve. "Intelligence Expertise in the Age of Information Sharing: Public–Private 'Collection' and Its Challenges to Democratic Control and Accountability." *Intelligence and National Security* 33, no. 1 (2018): 21–35. https://doi.org/10.1080/02684527.2017.1316956.

Popescul, Daniela and Laura D. Radu. "Data Security in Smart Cities: Challenges and Solutions." *Informatica Economica; Bucharest* 20, no. 1 (January, 2016): 29–38. http://dx.doi.org/10.12948/issn14531305/20.1.2016.03.

Posner, Richard, A. "an economic theory of privacy." *AEI journal on government and society* (2008): 19–26. https://doi.org/10.1017/cbo9780511625138.016.

Privacy International and IT-Political Association of Denmark. *The Right to Privacy in Denmark.* 24th Session. London: Privacyinternational.org, 2015. https://privacyinternational.org/sites/default/files/2017-12/Denmark_PI_UPR%20Stakeholder_submission_FINAL.pdf.

Privacy International. *The Right to Privacy in Singapore.* 24th session. London: Privacyinternational.org, 2015. https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf.

Puron-Cid, Gabriel. "Trust Measures for Implementers of E-Government Adoption: A Confirmatory Factor Analysis," 2013, 79–104.

Pushaw, Robert J., Jr. "Justiciability and Separation of Powers: A Neo-Federalist Approach." *Cornell Law Review* 81, no. 2 (January 1996): 393–512, https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2592&context=clr.

Raj, Pethuru, and Anupama C. Raman. *Intelligent Cities : Enabling Tools and Technology*. Boca Raton, Florida: CRC Press, 2015. https://doi.org/10.1201/b18561.

Reddick, Christopher G., *Comparative E-Government*. New York, NY: Springer New York, 2010. https://doi.org/10.1007/978-1-4419-6536-3.

Rengel, Alexandra. *Privacy in the 21st Century*. Leiden: Martinus Nijhoff Publishers, 2013. ProQuest.

Ross, Jamie, Fiona Stevenson, Rosa Lau, and Elizabeth Murray. "Factors That Influence the Implementation of E-Health: A Systematic Review of Systematic Reviews (an Update)." *Implementation Science* 11, no. 1 (December 2016): 146. https://doi.org/10.1186/s13012-016-0510-7.

Rüdiger, Mogens. "The 1973 Oil Crisis and the Designing of a Danish Energy Policy." *Historical Social Research Historische Sozialforschung,* 39, no. 4 (January, 2014): 94–112. http://doi.org/10.12759/hsr.39.2014.4.94-112.

Rule, James B. *Privacy in Peril*. Oxford; Oxford University Press, 2007.

"The Rule Of Law And The Singapore Constitution." April 25, 2019. https://www.supremecourt.gov.sg/news/events/magna/the-rule-of-law-and-the-singapore-constitution.

Rychla, Lucie. "Danish Police Allowed to Scan Thousands of License Plates." *Online Post,* January 12, 2016. http://cphpost.dk/news/danish-police-allowed-to-scan-thousands-of-licence-plates.html

"Safe_Cities_Index_2017_ENG.Pdf." Accessed July 13, 2019. https://www.nec.com/en/global/ad/campaign/safecitiesindex/pdf/Safe_Cities_Index_2017_ENG.pdf.

Saxena, N. C. *The Singapore Public Service and National Development: Virtuous Cycles*. Singapore: Ministry of Foreign Affairs Singapore, 2012. http://www.mfa.gov.sg/content/dam/mfa/images/media_center/MFA_CSC_UNDP_book/Virtuous_Cycles.pdf.

Schmeida, Mary and Ramona Mcneal. "Bridging the Inequality Gap to Accessing Medicare and Medicaid Information Online: An Empirical Analysis of E-Government Success 2002 through 2010*." In E-government success around the world cases, empirical studies, and practical recommendations,* edited by Gil Garcia, Jose Ramon, 60–78. Hershey, PA : Information Science Reference, an imprint of IGI Global, 2013.

"Security in Denmark - DLA Piper Global Data Protection Laws of the World." Accessed July 17, 2019. https://www.dlapiperdataprotection.com/index.html?t=security&c=DK.

Shah, Chirag. *Collaborative Information Seeking The Art and Science of Making the Whole Greater than the Sum of All*. The Information Retrieval Series, 34. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-28813-5.

"Singapore," October 27, 2015. https://freedomhouse.org/report/freedom-net/2015/singapore.

"Singapore Technical Paper - ECitizen Portal.Pdf." Accessed July 12, 2019. http://www.moha.gov.la/accsm/resources/Singapore/Singapore%20Technical%20Paper%20-%20eCitizen%20Portal.pdf.

"Singapore_2013_AnnexA.Pdf." Accessed July 13, 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Singapore_2013_AnnexA.pdf.

"Singapore-Baseline-Study.Pdf." Accessed July 12, 2019. https://www.article19.org/data/files/pdfs/publications/singapore-baseline-study.pdf.

Smart Cities : Foundations, Principles, and Applications. Hoboken, New Jersey: John Wiley & Sons, 2017. https://doi.org/10.1002/9781119226444.

"Smart City Network | Smart Aarhus." Accessed July 13, 2019. https://www.smartaarhus.eu/projects/smart-city-network.

Smart Nation and Digital Government Office. *Annex A Strategic National Projects for a SmartNation.* Singapore: Smart Nation and Digital Government Office, 2019. https://www.tech.gov.sg/files/media/media-releases/2017/08/Annex%20A%20StrategicNationalProjectsforaSmartNation.pdf.

Starr, Paul. *Liberalism and the Discipline of Power* in *Freedom's Power: The True Force of Liberalism.* Basic Books: 2007. Princeton.edu.

State of Green. *Smart Cities - Creating Livable, Sustainable And Prosperous Societies*. Version 1.0. Denmark: State of Green, 2018. https://stateofgreen.com/en/uploads/2018/05/Smart-Grid.pdf?time=1546533259.

Stephens, Kathryn. "U.S. Smart Grid Security: How Are We Doing?," 2011. http://www.nsci-va.org/WhitePapers/2011-10-19-SmartGrid%20Security-Stephens.pdf.

Stupp, Catherine. "Cambridge Analytica harvested 2.7 million Facebook users' data in the EU." *EURACTIV.COM. Ltd*, April 6, 2018. https://www.euractiv.com/section/data-protection/news/cambridge-analytica-harvested-2-7-million-facebook-users-data-in-the-eu/.

The SusNordic Gateway. “Denmark - National Policies for sustainable development.” October 20, 2008. http://folk.uio.no/kristori/prosus/susnordic/denmark/national_policies/index.html.

Tan, Carlton. “Lee Kuan Yew Leaves a Legacy of Authoritarian Pragmatism.” *The Guardian*, March 23, 2015. https://www.theguardian.com/world/2015/mar/23/lee-kuan-yews-legacy-of-authoritarian-pragmatism-will-serve-singapore-well.

Tham, Yuet M. ”Singapore.” In *The Privacy Data Protection And Cybersecurity Law Review Fifth Edition*, edited by Alan C. Raul, 287–303. (United Kingdom: Law Business Research Ltd, 2018). https://thelawreviews.co.uk//digital_assets/b5f160ac-fb67-48da-be84-a085ee98b2f2/The-Privacy-Data-Protection-and-Cybersecurity-Edition-5.pdf.

U.S. Congress. House. Committee on the Judiciary. *Warrantless Surveillance and the Foreign Intelligence Surveillance Act : The Role of Checks and Balances in Protecting American’s Privacy Rights. Pt. II : Hearing before the Committee on the Judiciary, House of Representatives.* 110 Cong., 1st sess., September 18, 2007.

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Privacy, Technology and the Law, author. *What Facial Recognition Technology Means for Privacy and Civil Liberties Hearing before the Subcommittee on Privacy, Technology and the Law of the Committee on the Judiciary, United States Senate, One Hundred Twelfth Congress, Second Session, July 18, 2012.* S. Hrg. ; 112–851. Washington: U.S. Government Printing Office, 2012.

United States, Office of the Director of National Intelligence, *Domestic Approach to National*. Washington, D.C.: Office of the Director of National Intelligence, 2016. https://www.dni.gov/files/documents/Newsroom/DomesticApproachtoNationalIntelligence.PDF.

Vibert, Frank. *The Rise of the Unelected: Democracy and the New Separation of Powers*. Cambridge, United Kingdom: Cambridge University Press, 2007. ProQuest.

Vile, M. J. C. *Constitutionalism and the Separation of Powers*. 2nd ed. Indianapolis: Liberty Fund, 1998. Liberty Fund, Inc.

World Population Review. “Developed Countries List 2019.” World Population Review, October 4, 2019. http://worldpopulationreview.com/countries/developed-countries/.

Yi, Seow Bei. “Parliament: Strict Regime to Ensure Data Privacy in Police Camera Footage; 5,000 Cameras Already Installed.” *The Straits Times*, February 6, 2018. https://www.straitstimes.com/politics/parliament-strict-regime-to-ensure-data-privacy-in-police-camera-footage-5000-cameras.

Ylijoki, Ossi, and Jari Porras. “Perspectives to Definition of Big Data: A Mapping Study and Discussion.” *Journal of Innovation Management* JIM 4, no. 1, (May 2016): 69–91. https://doi.org/10.24840/2183-0606_004.001_0006.

Zheng, Lei. “Developing E-Government Readiness Factors: A Bottom-Up Approach.” In *E-Government Success around the World: Cases, Empirical Studies, and Practical Recommendations,* ed. J. Ramon Gil-Garcia, 132–144. Hershey, PA : Information Science Reference, an imprint of IGI Glob, 2013. https://doi.org/10.4018/978-1-4666-4173-0.ch007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California