Smart Cities, Big Data, and the Resilience of Privacy

JANINE S. HILLER* AND JORDAN M. BLANKE**

Smart Cities are designed to ubiquitously collect information about people, places, and activities and to use that data to provide more efficient services and to build resilience against disasters. Projects like the Rockefeller Foundation-funded "100 Resilient Cities" are exploring how big data can be used to design and strengthen resilience in cities around the world. Large technology companies are helping to design and secure components of the Internet of Everything, which is part of a smart city structure. Relationships between governments and citizens, as well as between individuals and businesses, will see substantial changes due to this rapidly expanding collection and use of potentially intimate information. In this dynamic environment, it is difficult to protect privacy under traditional principles that did not anticipate a sensor-connected, surveillance-laden, data-driven world of the smart city. Slow moving court cases and inflexible fair information privacy practices may be insufficient to limit and/or guide smart city implementation that respects individual privacy. Cities need a methodology that will enable a discussion of how law, regulation, and social norms can respond to the dynamic disruption that a smart city poses to the fundamental nature of privacy.

This Article proposes that resilience theory can be a useful lens for this analysis. Resilience theory has multidisciplinary roots in engineering, biology, ecology, and sociology, and is generally understood as a way to understand how systems react to extreme pressures—whether they decline and die, or whether they adapt and thrive. The theory is used to describe multiple aspects of systems and organisms, from the ability of a building to withstand an earthquake to the ability of an organism not only to survive, but to also evolve into a different and possible better state. This Article views privacy as a system and examines it through the resiliency lens, framing the question of how privacy can adapt and survive in a smart city.

[*] R. E. Sorensen Professor of Finance, Professor of Business Law, Pamplin School of Business, Virginia Tech, Blacksburg, Virginia.

[**] Ernest L. Baskin, Jr. Distinguished Professor of Computer and Information Systems and Law, Stetson School of business & Economics, Mercer University, Atlanta, Georgia.

The Authors thank the participants in the 2015 Law and Ethics of Big Data Colloquium in Bloomington, Indiana, sponsored by Virginia Tech, Center for Business Intelligence and Analytics, Pamplin College of Business and Indiana University, Department of Legal Studies; the participants at the 2015 Privacy Law Scholars Conference in Berkeley, California, sponsored by the Berkeley Center for Law & Technology and the George Washington University Law School; and the participants in the 2016 Law and Ethics of Big Data Colloquium in Indianapolis, Indiana, sponsored by Virginia Tech, Center for Business Intelligence and Analytics, Pamplin College of Business and Indiana University, Department of Legal Studies. In particular, the Authors thank the above-mentioned conference participants for their helpful comments. The Authors also thank Elizabeth C. Brown, MBA 2015 Stetson School of Business & Economics, Mercer University, Atlanta, Georgia, for her excellent research assistance.

Table of Contents

Introduction

> In a fully "smart" city, every movement an individual makes can be tracked. The data will reveal where she works, how she commutes, her shopping habits, places she visits and her proximity to other people. . . . [T]his data will be centralized and easy to access. . . . Private companies could know more about people than they know about themselves.
> —Mike Weston[1]

[1] Mike Weston, *'Smart Cities' Will Know Everything About You*, Wall St. J. (July 12, 2015, 6:36 PM), http://www.wsj.com/articles/smart-cities-will-know-everything-about-you-1436740596. Weston is the CEO of a data consulting company. *Id.*

A sensor-strapped, mobile-manipulated, Internet-integrated smart city is quickly becoming a reality in urban centers around the world. The data-driven city depends on data collected from buildings, infrastructure, people, and third-party data brokers. Government agencies, quasi-governmental utilities, commercial interests, and others will trace, analyze, and predict the movements, needs, and scarcities of citizens in the city in order to manage resources and protect the community most effectively. But while individuals may have some vague inkling that information is being collected about them, they are probably unaware of the extent of the information that is or will be collected on a daily basis by their water company, their electric company, their gas company and others, and by the many agencies and departments of their city, county, state, and federal governments. Relationships between governments and citizens, as well as between individuals and businesses, will see substantial changes due to this rapidly expanding collection and use of potentially intimate information. A fundamental question demanding equally expansive and immediate attention is whether personal information protection or privacy can survive amidst these disruptive changes, and whether law and regulation can effectively support its survival.

Several prominent global projects depend upon the use of big data to pursue sustainability for cities, efficiently provide fundamental public services, increase citizen engagement, and strengthen public security.[2] Urban designers and planners use big data to address concerns about not only the environment, city infrastructures, floods and other disasters, but increasingly to address broader socioeconomic aspects of overall city and population health.[3] The Rockefeller Foundation funds the ambitious "100 Resilient Cities" project,[4] and the United Nations Global Pulse is exploring how big data can be used to build smart cities in developing and emerging regions of the world.[5] Large technology companies, like Microsoft and Cisco, are helping to design the structure and security of the Internet of Everything[6] that is so fundamental to smart cities. Importantly, data-driven analytics provides key information for understanding citizen and environmental relationships, which in turn drive sustainable decisions and build urban survivability. While there are

[2] *See infra* Part I.

[3] *Id.*

[4] *See infra* note 87.

[5] *See* Simone Sala, *Building Resilient Cities in Developing and Emerging Regions Via Big Data*, UNITED NATIONS GLOBAL PULSE (Jan. 5, 2015), http://www.unglobalpulse.org/blog/building-resilient-cities-developing-and-emerging-regions-big-data; *see also* Giulio Quaggiotto, *Combining "Big" and "Small" Data to Build Urban Resilience in Jakarta*, UNITED NATIONS GLOBAL PULSE (Apr. 9, 2014), http://www.unglobalpulse.org/urban-resilience-petajakarta (including an interview with the Directors of PetaJakarta.org, describing a project in Indonesia).

[6] *See infra* Part I.

many definitions of "big data," most describe the collection, storage, use, and reuse of vast amounts of data—that which is both personally identifiable and anonymous—collected by both public and private entities from databases, the Internet, smart phones, and increasingly by sensor devices of every shape, form, and flavor.[7] Ultimately, the smart city of tomorrow will make big data of today look small.

Many advantages come from the collection of data described above, but there are also grave threats to individual privacy. Big data and surveillance poses "substantial risks of inappropriate constructions of smart cities and the human societies living in them."[8] The smart city's pervasive use of sensors and citizen surveillance threatens to create a society that ignores boundaries for individual privacy. In fact, individual privacy may not survive in a smart city where every movement is tracked, compared with everyone else's movements, combined with vast troves of individually identified data, and immediately used to "nudge" behaviors.[9] In the eyes of some, this is a potentially "terrifying"[10] vision of a smart city, replete with endless sensors, a community without individual rights to privacy, as the dynamic use of surveillance technology, data retention, analytics, and predictive methodologies combine to eradicate traditional notions of privacy.

Yet, smart cities are the future. Climate change, population movements, and disruptive events demand them. The White House announced a major policy program and financial investment in smart cities in September 2015.[11] One hundred sixty million dollars is slated for funding research, with cities, universities, and private industry all taking part in the initiative.[12]

In this dynamic, fast moving environment, it is difficult to protect privacy by means of existing laws and self-regulatory practices that were not written in anticipation of the sensor-connected, surveillance-laden, data-driven world of the future smart city. Slow moving court cases and inflexible fair information privacy practices may be insufficient to limit or guide the tsunami of smart city implementation. A methodology is necessary to analyze the way law, regulation, and norms can keep up with the dynamic disruption that a smart city poses to the fundamental

[7] *Id.*

[8] *See* Sala, *supra* note 5.

[9] *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008) (proposing that individuals can be nudged through choice architecture to act in certain ways without compromising their freedom of choice).

[10] *See* Weston, *supra* note 1.

[11] Dan Correa, *Launching a Smart Cities Initiative to Tackle City Challenges with Innovative Approaches*, THE WHITE HOUSE (Sept. 16, 2015, 3:03 PM), https://www.whitehouse.gov/blog/2015/09/16/launching-smart-cities-initiative-tackle-city-challenges-innovative-approaches.

[12] *Id.*

nature of privacy. This Article proposes that resilience theory is a useful lens for this analysis.

Resilience theory has multidisciplinary roots in the engineering,[13] biological,[14] and ecological[15] disciplines, and is generally understood as a way to understand how systems react to extreme pressures—whether they decline and die, or whether they adapt and thrive.[16] It is used to describe multiple aspects of systems and organisms; from the ability of a building to withstand an earthquake to the ability of an organism not only to survive, but also to evolve to a better defensive state after illness.[17] The Stockholm Resilience Center defines resilience as "the capacity of a system . . . to deal with change and continue to develop."[18] Furthermore, the goal of resilience studies is to understand ways to build in or obtain resilience.[19] The opposite of resilience is brittleness.[20] Brittleness means that the subject can withstand a limited amount of stress before it will break, and it implies that it cannot "bounce back" from its brokenness.[21]

Thus, this Article adopts the paradigm that privacy is the system studied and is defined by laws and norms. The disruption to privacy is defined as the extensive information collection by big data methodologies and surveillance in the smart city. Under resilience analysis that is described in detail in Part III, we analyze whether privacy in the smart city has the capacity to adapt and evolve to survive, or whether the way

[13] *See* C. S. Holling, *Engineering Resilience Versus Ecological Resilience*, *in* NAT'L ACAD. OF ENG'G, ENGINEERING WITHIN ECOLOGICAL CONSTRAINTS 31, 36–38 (Peter C. Schulze ed., 1996); Azad M. Madni & Scott Jackson, *Towards a Conceptual Framework for Resilience Engineering*, 3 IEEE SYS. J. (SPECIAL ISSUE) 181, 181 (2009) ("[R]esilience engineering is a proactive approach that looks for ways to enhance the ability of organizations to explicitly monitor risks . . . .").

[14] *See* Adriana Feder et al., *Psychobiology and Molecular Genetics of Resilience*, 10 NATURE REVS. NEUROSCIENCE 446 (2009) (discussing initial studies of children and their ability to persevere despite severe stress).

[15] *See* C. S. Holling, *Resilience and Stability of Ecological Systems*, 4 ANN. REV. ECOLOGY & SYSTEMATICS 1 (1973).

[16] Fridolin Simon Brand & Kurt Jax, *Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object*, 12 ECOLOGY AND SOC'Y 23, 24–26 (2007) (providing ten different definitions of resilience from different disciplines).

[17] *See infra* Part III; *see also* Arjen Boin & Michel J. G. van Eeten, *The Resilient Organization: A Critical Appraisal*, 15 PUB. MGMT. REV. 429, 431 (2013) (describing two different models of resilience).

[18] *What Is Resilience? An Introduction to a Popular Concept*, STOCKHOLM RESILIENCE CTR., http://www.stockholmresilience.org/research/research-news/2015-02-19-what-is-resilience.html (last visited Jan. 16, 2017).

[19] *See* Richard Haigh & Dilanthi Amaratunga, *An Integrative Review of the Built Environment Discipline's Role in the Development of Society's Resilience to Disasters*, 1 INT'L J. DISASTER RESILIENCE BUILT ENV'T 11, 14 (2010) ("The objective is to build resilience by maximising the capacity to adapt to complex situations." (internal citation omitted)).

[20] *See* Bryan G. Norton, *A Scalar Approach to Ecological Constraints*, *in* NAT'L ACAD. ENG'G, ENGINEERING WITHIN ECOLOGICAL CONSTRAINTS 45, 53 (Peter C. Schulze ed., 1996) (describing a theory that systems can be overcome and unable to respond, becoming brittle and collapsing).

[21] *See* Paulina Aldunce et al., Research Paper, *Framing Disaster Resilience: The Implications of the Diverse Conceptualisations of "Bouncing Back*,*"* 23 DISASTER PREVENTION & MGMT. 252, 262–63 (2014) (discussing variations of the concept of bouncing back from disturbances).

that we define our fundamental right to privacy in laws and norms is brittle, and will ultimately break and fail to survive under the disruption of ubiquitous and opaque surveillance in the smart city.

This Article first describes what makes a city "smart," including the many ways in which data is collected and utilized within existing and future cities. Smart cities are briefly compared to resilient cities, but for purposes of this Article, the terms are used as generally equivalent terms. Theories of resilience are discussed as possible approaches to conceive of and protect privacy in smart cities. Lastly, the Article discusses the National Institute of Standards and Technology Privacy Framework as a systems-based method to approach privacy management. While the framework advances adaptability for preserving privacy, it lacks opportunities for social discourse and other elements necessary for the evolution and resilience of privacy. This Article contributes to the privacy literature in two ways: (1) by discussing the impact of smart cities on privacy; and (2) by placing the privacy conversation within the paradigm and disciplinary analysis of resilience theory.

I. Big Data and Smart Cities

According to a May 2014 report from the Executive Office of the President, most definitions of "big data" "reflect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data. In other words, 'data is now available faster, has greater coverage and scope, and includes new types of observations and measurements that previously were not available.'"[22] The report defined big data as "large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future."[23]

Big data is created in smart cities because of the technology and applications used to collect and analyze personal information from citizens and residents that is shared across functional areas and used in

[22] Exec. Office of the President, Big Data: Seizing Opportunities, Preserving Values 2 (2014) (quoting Liran Einav & Jonathan D. Levin, *The Data Revolution and Economic Analysis* (Nat'l Bureau of Econ. Research, Working Paper No. 19035, 2013), http://www.nber.org/papers/w19035); *see also* Julie Brill, Essay, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 Fordham L. Rev. 205, 206 nn.1–3 (2014) (discussing estimates that in 2011, 1.8 gigabytes of data was created, primarily by individuals, and that the amount of total data in existence will double every two years); Joseph Jerome, *Big Data: Catalyst for a Privacy Conversation*, 48 Ind. L. Rev. 213, 214, nn.10–13 (2014) (discussing extent of data collection).

[23] *See* Exec. Office of the President, *supra* note 22, at 3 (quoting Nat'l Sci. Found., Core Techniques and Technologies for Advancing Big Data Science & Engineering 5 (2012), http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf).

the urban planning process.[24] Therefore, a brief discussion of the broader societal context in which personal data is collected and aggregated is warranted, followed by a description of specific collection and use of data in smart cities.

Big data is capable of delivering many potential benefits. In the area of healthcare, for example, major improvements have been made because of the ability to mine and analyze huge datasets, aiding in determining drug interactions, identifying negative side effects to specific drugs, and discovering advantages from certain drug therapies.[25] In cities, electricity service providers can use big data within a "smart grid" to better control and monitor usage.[26] Urban planners can use big data to improve decisionmaking regarding road and mass transit traffic patterns and to better plan for future improvements to the infrastructure.[27] However, there are big concerns about big data, including the incredible amount of information—both accurate and potentially inaccurate—that can be generated by the use of predictive analysis applied to that data.[28] Narratives about both the present and the future are legend. Nearly everyone knows about Target's accurate prediction of a teenage girl's pregnancy before her family even knew, and many are familiar with the futuristic story line from the film *Minority Report* about the PreCrime division of a future police department that apprehends criminals before they have a chance to perpetrate their "crimes."[29] These predictions, real and not so futuristic, are possible because of widespread data collection from devices that are connected to people and places, creating what is known as the "Internet of Things."

A. The Internet of Things

In recent years there has been a proliferation of devices capable of collecting and transmitting information to the Internet and to databases.[30] These devices basically make up the so-called "Internet of Things,"[31] or the "Internet of Everything."[32] Massive amounts of data are collected

[24] *See* Michael Batty, *Big Data, Smart Cities and City Planning*, 3 Dialogues Hum. Geography 274, 277 (2013).

[25] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 245–47 (2013).

[26] *Id.* at 248.

[27] *Id.*

[28] *Id.* at 251–55.

[29] *Id.* at 253.

[30] *See* Christina Scelsi, *Care and Feeding of Privacy Policies and Keeping the Big Data Monster at Bay: Legal Concerns in Healthcare in the Age of the Internet of Things*, 39 Nova L. Rev. 391, 393 (2015).

[31] Scott Peppet notes that the term is generally attributed to Kevin Ashton, dating back to a presentation in 1999. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 89 n.13 (2014).

[32] This term is attributed to Cisco CEO John Chambers. *Id.* at 89 n.14.

from seemingly everywhere—from cell phones to cars to underwear.[33] And rather than existing as a mere fleeting shadow or grain of sand, this data is meticulously collected, stored, sold, manipulated, repurposed and reused. There are a great variety of devices today—mostly sensors—that generate an enormous volume of (largely unregulated) data.[34] And, "[o]nce filtered through 'Big Data' analytics, these data are the grist for drawing revealing and often unexpected inferences about habits, predilections, and personalities."[35]

Smart phones now contain a wide variety of sensors. Most have a compass, an accelerometer, an ambient light monitor, a proximity sensor, a gyroscope, a GPS device, a microphone, and often multiple cameras.[36] Numerous studies have demonstrated how data from these sensors is aggregated and analyzed to "infer a user's mood, stress levels, personality type, bipolar disorder, demographics . . . , smoking habits, overall well-being, progression of Parkinson's disease, sleep patterns, happiness, levels of exercise, and types of physical activity or movement."[37]

Additionally, the concepts of "data fusion" or "sensor fusion" refer to the phenomenon of data collected from a variety of different sources being combined to create more information and more powerful inferences than can be produced by the separate sources.[38] This phenomenon will become even more important with the proliferation of the many varieties of sensors that will be connected in the smart cities.

B. Smart Cities

Definitions of a smart city include references to the collection of data from many sources, especially from embedded sensors, to better plan for and coordinate the wide variety of activities occurring in urban

[33] Researchers at the University of Arkansas developed a system that "features tiny wireless nanostructured, textile sensors—ideal for a sportsbra or a vest for men—which collects heart rate and health stats and sends them directly to your smartphone for data-crunching." *New 'E-Bra' Tracks Health Stats and Sends Them to Your Smartphone*, DAILY NEWS (May 11, 2012, 1:14 PM), http://www.nydailynews.com/life-style/health/new-e-bra-tracks-health-stats-sends-smartphone-replace-conventional-blood-pressure-monitors-article-1.1076442. Ariana Eunjung Cha, *The Human Upgrade: The Revolution Will Be Digititized*, WASH. POST (May 9, 2015), http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/. It is estimated that ten million units of smart garments will be sold in 2015 and that this number will increase to more than fifty million by 2020. Scelsi, *supra* note 30, at 393 n.5.

[34] *See* Peppet, *supra* note 31, at 98–116. ARM and IBM recently announced the release of an Internet of Things starter kit that will enable hobbyists or small businesses to get data from "the on board sensors into the IBM cloud within minutes of opening the box." Agam Shah, *ARM, IBM Offer Starter Kit for Making IOT Devices*, PCWORLD (Feb. 23, 2015, 8:10 PM), http://www.pcworld.com/article/2888132/arm-ibm-offer-starter-kit-for-making-iot-devices.html.

[35] *See* Peppet, *supra* note 31, at 90 (internal citations omitted).

[36] *Id.* at 114–15.

[37] *Id.* at 115–16 (internal citations omitted).

[38] *Id.* at 121–22.

environments.[39] Many "[c]onsulting and IT firms propound a tech-centric approach to smart cities."[40] IBM defines a "smarter city" as "one that makes optimal use of all the interconnected information available today to better understand and control its operations and optimize the use of limited resources."[41] Cisco defines a "smart city" as one that adopts "scalable solutions that take advantage of information and communications technology (ICT) to increase efficiencies, reduce costs, and enhance quality of life."[42] One advisory firm lists eight elements that define a smart city: (1) smart governance; (2) smart building; (3) smart healthcare; (4) smart mobility; (5) smart infrastructure; (6) smart technology; (7) smart energy; and (8) smart citizens.[43] While no city has all of these, predictions are that by 2025 at least twenty-six global smart cities will operate at least five of these parameters.[44]

1. Prototype Cities

Santander, a small port city in Spain,[45] is an early prototype of a smart city. The smart city project included the installation of about 12,000 sensors "under the asphalt, affixed to street lamps and atop city buses."[46] The sensors are designed to measure air pollution, locate available parking spaces, automatically dim street lights, and even tell garbage collectors when trash cans are full.[47] Street signs are equipped with digital panels that display real-time parking information and relay the information to a central control center.[48] Residents can download a suite of smartphone applications to receive current information on parking, road closures, bus

[39] *See, e.g.*, Courtney Humphries, *The Too-Smart City*, BOSTON GLOBE (May 19, 2013), http://www.bostonglobe.com/ideas/2013/05/18/the-too-smart-city/q87J17qCLwrN90amZ5CoLI/story.html ("[T]he 'smart city'—a wired, sensor-filled streetscape that uses cloud computing and sophisticated software to transform cities into intelligent machines that adapt to people's lives and steer behavior.").

[40] Goutam Das & Manu Kaushik, *A Tale of 100 Smart Cities: The Quest to Build Them and the Problems on the Way*, BUS. TODAY (Mar. 15, 2015), http://businesstoday.intoday.in/story/challenges-the-govt-faces-in-building-100-smart-cities-india/1/215950.html.

[41] MICHAEL COSGROVE ET AL., SMARTER CITIES SERIES: INTRODUCING THE IBM CITY OPERATIONS AND MANAGEMENT SOLUTION 1 (2011).

[42] GORDON FALCONER & SHANE MITCHELL, SMART CITY FRAMEWORK: A SYSTEMATIC PROCESS FOR ENABLING SMART+CONNECTED COMMUNITIES 2 (2012); *see Smart Cities*, CAPITAL CITY COMMITTEE: ADELAIDE (May 2014) (describing three categories of smart city definitions; broad, data-driven, and citizen-focused).

[43] Liz Enbysk, *New Reports Highlight Smart Security, Smart Citizens and Smart City Essentials*, SMART CITIES COUNCIL (Nov. 14, 2014, 6:00 AM), http://smartcitiescouncil.com/article/new-reports-highlight-smart-security-smart-citizens-and-smart-city-essentials.

[44] *Id.*; *see* Das & Kaushik, *supra* note 40.

[45] *See* Lauren Frayer, *High-Tech Sensors Help Old Port City Leap into Smart Future*, NAT'L PUB. RADIO (June 4, 2013, 3:27 AM), http://www.npr.org/blogs/parallels/2013/06/04/188370672/Sensors-Transform-Old-Spanish-Port-Into-New-Smart-City.

[46] *Id.*

[47] *Id.*

[48] *Id.*

delays, and pollen counts.[49] The city has saved about twenty-five percent on its electricity costs and twenty percent on garbage collection.[50]

The project, which took about three years to complete—from 2010 through 2013—eventually installed approximately 15,000 sensors in an area of about 13.4 square miles.[51] The completed system has been likened to the role-playing video game SimCity: "The City Council is able to see, at any time, a snapshot of the entire network of sensors."[52] This enables city officials with a real-time view "to make better decisions and engage in more cost-effective planning."[53] An expanded project, SmartSantander, aims to deploy this system in some other European cities.[54] A description of the project provides:

> SmartSantander proposes a[n] . . . experimental research facility in support of typical applications and services for a smart city. This unique experimental facility will be sufficiently large, open and flexible to enable horizontal and vertical federation with other experimental facilities and stimulates development of new applications by users of various types including experimental advanced research on IoT technologies and realistic assessment of users' acceptability tests. The project envisions the deployment of 20,000 sensors in Belgrade, Guildford, Lübeck and Santander (12,000), exploiting a large variety of technologies.[55]

Libelium, the company that made the sensor networks for Santander,[56] created a graphical illustration of its view of a "smart city" or "future city" called "Libelium Smart World."[57] It highlights a wide collection of functions, operations, properties, and characteristics of this vision, including surveillance and predictions about the functions of systems as varied as water quality and golf courses.[58]

[49] *Id.*

[50] *Id.*

[51] Francisco Jariego, *The Real Sim City: How over 15,000 Sensors Made Santander Smart*, TELECOMS TECH (Mar. 26, 2014, 4:04 PM), http://www.telecomstechnews.com/news/2014/mar/26/real-sim-city-how-over-15000-sensors-made-santander-smart2/.

[52] *Id.*

[53] *Id.*

[54] *See* SMARTSANTANDER, http://www.smartsantander.eu/ (last visited Jan. 16, 2017).

[55] *Id.*

[56] *See* Alberto Bielsa, *Wireless Applications: The Smart City Project in Santander*, SENSORS ONLINE (Mar. 1, 2013), http://www.sensorsmag.com/wireless-applications/smart-city-project-santander-11152 (describing specifications for the sensors and networks used in the Santander project).

[57] Jacob Morgan, *Cities of the Future: What Do They Look Like, How Do We Build Them and What's Their Impact?*, FORBES (Sept. 4, 2014, 12:08 AM), http://www.forbes.com/sites/jacobmorgan/2014/09/04/cities-of-the-future-what-do-they-look-like-how-do-we-build-them-and-whats-their-impact/#78dd0d6a4e9b.

[58] *Id.* The entire list includes the following: Air Pollution, Forest Fire Detection, Wine Quality Enhancing, Offspring Care, Sportsmen Care, Structural Health, Quality of Shipment Conditions, Smartphone Detection, Perimeter Access Control, Radiation Levels, Electromagnetic Levels, Traffic Congestion, Water Quality, Waste Management, Smart Parking, Golf Courses, Smart Roads, Smart Lighting, Intelligent Shopping, Noise Urban Maps, Water Leakages, Vehicle Auto-diagnosis, and Item Location. *Id.*

The South Korean city of Songdo is unique because it was created anew as a smart city; twelve years ago Songdo was a barren mudflat.[59] Now, forty billion dollars and a dozen years later, the joint venture by Cisco and real estate developers has resulted in a so-called "City of the Future" or "The World's Smartest City," home to about 70,000 people.[60] The city has completed about sixty percent of its planned infrastructure and buildings, and its population is about one-third of the total expected when the project is set to be completed in 2018.[61] There are numerous sensors that monitor everything from temperature to energy use to traffic flow.[62] Environmental planning efforts include charging stations for electric cars and a water recycling system that separates clean drinking water from the water that is used to flush toilets.[63] Household waste is disposed directly from homes into underground tunnels, where it is automatically processed and treated.[64]

Although these cities embraced smart urban systems comprehensively, many cities around the world are even "smarter" in specific areas: Amsterdam focuses on energy savings;[65] Barcelona partnered with Cisco to implement Cisco's vision of the Internet of Everything;[66] Rio de Janeiro, largely in anticipation of the 2014 World Cup and the 2016 Summer

[59] *See* Wendy Tanaka, *Cities of the Future: Songdo, South Korea—Roadmap for a New Community*, CISCO THE NETWORK (Apr. 25, 2012), http://newsroom.cisco.com/feature/776681/Cities-of-the-Future-Songdo-South-Korea-Roadmap-for-a-New-Community.

[60] *See* Ross Arbes & Charles Bethea, *Songdo, South Korea: City of the Future?*, ATLANTIC (Sept. 27, 2014), http://www.theatlantic.com/international/archive/2014/09/songdo-south-korea-the-city-of-the-future/380849/; Morgan, *supra* note 57.

[61] *See* Arbes & Bethea, *supra* note 60; Morgan, *supra* note 57.

[62] *See* Lucy Williamson, *Tomorrow's Cities: Just How Smart Is Songdo?*, BBC NEWS (Sept. 2, 2013), http://www.bbc.com/news/technology-23757738.

[63] *Id.*

[64] *Id.*

[65] Amsterdam Smart City has a collection of projects whose goals include reducing carbon dioxide emissions, maximizing efficient use of electricity for street lighting and home consumption, diminishing traffic, improving waste collection, improving air quality, reducing noise, employing sustainable strategies, and using alternative energy sources. AMSTERDAM SMART CITY, http://amsterdamsmartcity.com/projects (last visited Jan. 16, 2017) (providing a multitude of projects available on their website); *see* Das & Kaushik, *supra* note 40 (comparing Barcelona's success to first smart cities in India); Mark Scott, *Old World, New Tech: Europe Remains Ahead of U.S. in Creating Smart Cities*, N.Y. TIMES (Apr. 21, 2014), http://www.nytimes.com/2014/04/22/business/energy-environment/europe-remains-ahead-of-us-in-creating-smart-cities.html?_r=2 (explaining how public-private partnerships in Europe assist development of smart cities).

[66] *See* Maged N. Kamel Boulos & Najeeb M. Al-Shorbaji, *On the Internet of Things, Smart Cities and the WHO Healthy Cities*, 13 INT'L J. HEALTH GEOGRAPHICS 10, 11 (2014); SHANE MITCHELL ET AL., THE INTERNET OF EVERYTHING FOR CITIES: CONNECTING PEOPLE, PROCESS, DATA, AND THINGS TO IMPROVE THE 'LIVABILITY' OF CITIES AND COMMUNITIES 10 (2013). For a discussion of whether smart cities might go too far and an argument that citizens will keep them in check, see *Clever Cities: The Multiplexed Metropolis*, ECONOMIST (Sept. 7, 2013), http://www.economist.com/news/briefing/21585002-enthusiasts-think-data-services-can-change-cities-century-much-electricity.

Olympics, implemented several new programs;[67] and Boston implemented new systems to improve its transportation infrastructures and its ability to fight crime.[68] India has a goal of developing 100 smart cities,[69] as it anticipates that fifty percent of its citizens will live in cities by 2050 as compared to the thirty-two percent who presently live in such places. Yet, India recognizes that building a smart city is a daunting task.[70] Smart city projects in U.S. cities face similar challenges.[71]

2. *Smart City Projects in the United States*

Chicago's Array of Things ("AoT")[72] is a unique "network of interactive, modular sensor boxes that will be installed around Chicago to collect real-time data on the city's environment, infrastructure, and activity for research and public use."[73] The project is a joint initiative of the Argonne National Laboratory ("Argonne") and the University of Chicago.[74] The plan is to deploy fifty prototype sensor nodes in the summer of 2016, and to reach an installed base of 500 by the end of 2018.[75] Sensors in the prototype nodes will measure "temperature, barometric pressure, light, vibration, carbon monoxide, nitrogen dioxide, sulfur dioxide, ozone, ambient sound intensity, pedestrian and vehicle traffic, and surface temperature."[76] The collected data will help systems monitor air quality, sound and vibration (to detect heavy traffic), and temperature.[77] For example, data will help predict the need for road-

[67] *See* Federico Guerrini, *World's Top 7 Smart Cities of 2015 Are Not the Ones You'd Expect*, FORBES (Jan. 28, 2015, 11:53 AM) http://www.forbes.com/sites/federicoguerrini/2015/01/28/worlds-top-7-smartest-cities-of-2015-are-not-the-ones-youd-expect/.

[68] Boston uses acoustic sensors to detect and pinpoint the location of gunshots. The Massachusetts Bay Transportation Authority built an extensive network of thousands of surveillance cameras and installed special sensors to detect biological weapons. The Massachusetts Turnpike's EZPass can monitor the activity of anyone with a transponder installed on their windshields, automated license plate recognition technology can track any car in the city, and smart grad utility-monitoring systems collect detailed energy consumption information. *See* Humphries, *supra* note 39.

[69] *See* Das & Kaushik, *supra* note 40.

[70] *Id.*

> No less than eight ministries need to work together to build a smart city, says B.K. Sinha, Head of Civil Engineering at the Bureau of Indian Standards. These are the ministries of urban development, IT, power, road transport and highways, water resources, labour and employment, human resource development, and consumer affairs, food and public distribution. Policies at the central level are being framed by the urban development ministry but there is no single point clearing house for contacts private investors look for.

Id. at 46.

[71] *See* sources cited *infra* notes 72–83.

[72] *See* ARRAY OF THINGS, https://arrayofthings.github.io/ (last visited Jan. 16, 2017).

[73] *Id.*

[74] *See FAQ*, ARRAY OF THINGS, https://arrayofthings.github.io/faq.html (last visited Jan. 16, 2017).

[75] *Id.*

[76] *Id.*

[77] *See* ARRAY OF THINGS, *supra* note 72.

salting responses during storms, provide up-to-date "block-by-block" weather information, and suggest safe and efficient walking and driving routes.[78] A goal of the AoT project is to "provide data to help engineers, scientists, policymakers and residents work together to make Chicago and other cities healthier, more livable and more efficient."[79] All project data "will be open, free, and available to the public" and "software, hardware, parts, and specifications will also be published as open source."[80]

New York City is another large modern city that collects and monitors massive amounts of data on a daily basis for purposes ranging from planning to logistics to safety. For example, the New York City Police Department uses a Microsoft product called a "domain awareness system" to collect and analyze data from 3000 public surveillance cameras, 200 automatic license plate readers, 2000 radiation sensors, and numerous other police databases.[81] The system provides police with real-time information to track suspects and their cars, to detect unattended packages, to compare license plate numbers with watch lists, and to perform a variety of other policing activities.[82] The New York City Marathon was observed using these methods in 2013, in the aftermath of the Boston Marathon tragedy.[83]

C. "Resilient Cities"

The Rockefeller Foundation recently launched a project to create an organization called "100 Resilient Cities," which is "dedicated to helping cities around the world become more resilient to the physical, social, and economic challenges that are a growing part of the 21st century."[84] The Rockefeller Foundation itself was created in 1913 with a mission "to promote the well-being of humanity throughout the world."[85] It pursues its mission in part by "helping people, communities and institutions prepare for, withstand, and emerge stronger from acute shocks and chronic stresses."[86] Discussed in more detail in Part III, this is the essence of what it means for a system to be resilient: the ability to survive and improve in the face of both everyday and unusual challenges and threats. The organization named its first group of thirty-three resilient

[78] *Id.*

[79] *See FAQ*, *supra* note 74.

[80] *See* Array of Things, *supra* note 72.

[81] *See* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 Wash. L. Rev. 35, 48–49 (2014).

[82] *Id.*

[83] *Id.* at 49.

[84] *About Us*, 100 Resilient Cities, http://www.100resilientcities.org/about-us#/-_/ (last visited Jan. 16, 2017).

[85] *100 Resilient Cities & the Rockefeller Foundation: 37 New Member Cities, Reaching 100 City Milestone*, 100 Resilient Cities (May 24, 2016) http://www.100resilientcities.org/blog/entry/100-resilient-cities-and-the-rockefeller-foundation-announce-37-new-member#/-_/.

[86] *Id.*

cities in December 2013,[87] a second group of thirty-five additional cities in December 2014,[88] and a final group of thirty-seven additional cities in May 2016.[89] Each city received a one million dollar two-year grant, which included funding for a Chief Resilience Officer ("CRO").[90] In order to be effective, the CRO must (1) work "across government departments to help a city improve internal communications"; (2) bring "together a wide array of stakeholders to learn about a city's challenges and help build support for individual initiatives, and for resilience building in general"; (3) lead "the resilience strategy . . . to help identify the city's resilience challenges, its capabilities and plans to address them, and then to identify the gaps between these two"; and (4) act as a "resilience point person."[91]

While the 100 Resilient Cities project certainly has a different focus than some of the other smart city initiatives, for purposes of our discussion, we generally consider "Resilient Cities" a subset of "smart cities." Most of the privacy concerns will be similar, although perhaps heightened. That said, the Rockefeller Foundation and its "100 Resilient Cities" project are making notable contributions to the discussion surrounding protecting

[87] *See Selected Cities*, 100 RESILIENT CITIES, http://www.100resilientcities.org/cities#/-_/ (last visited Jan. 16, 2017). Click on the "all rounds" dropdown menu to select Round 1 of the first 100 cities, which include: Bangkok (Thailand), Berkeley (USA), Boulder (USA), Bristol (UK), Byblos (Lebanon), Christchurch (New Zealand), Da Nang (Vietnam), Dakar (Senegal), Durban (South Africa), El Paso (USA), Glasgow (UK), Jacksonville (USA), Los Angeles (USA), Mandalay (Myanmar), Medellín (Colombia), Melbourne (Australia), Mexico City (Mexico), New Orleans (USA), New York City (USA), Norfolk (USA), Oakland (USA), Porto-Alegre (Brazil), Quito (Ecuador), Ramallah (Palestine), Rio de Janeiro (Brazil), Rome (Italy), Rotterdam (Netherlands), San Francisco (USA), Semarang (Indonesia), Surat (India), and Vejle (Denmark). *Id.* Alameda (USA), Ashkelon (Israel), and Jacksonville (USA) were initially selected as part of a group of thirty-three cities, but lost their grants or were dropped after the initial designation. *Id.*

[88] *Id.* Click on the "all rounds" dropdown menu to select Round 2 of the first 100 cities, which include: Accra (Ghana), Amman (Jordan), Athens (Greece), Bangalore (India), Barcelona (Spain), Belgrade (Serbia), Boston (USA), Cali (Colombia), Chennai (India), Chicago (USA), Dallas (USA), Deyang (China), Enugu (Nigeria), Huangshi (China), Juárez (Mexico), Kigali (Rwanda), Lisbon (Portugal), London (United Kingdom), Milan (Italy), Montreal (Canada), Paris (France), Pittsburgh (USA), San Juan (USA), Santa Fe (Argentina), Santiago de los Caballeros (Dominican Republic), Santiago (Chile), Singapore (Singapore), St. Louis (USA), Sydney (Australia), Thessaloniki (Greece), Toyama (Japan), Tulsa (USA), Wellington (New Zealand). *Id.* Arusha (Tanzania) and Phnom Penh (Cambodia) were initially selected as part of a group of thirty-five cities, but lost their grants or were dropped after the initial designation. *Id.*

[89] *Id.* Click on the "all rounds" dropdown menu to select Round 3 of the first 100 cities, which include: Addis Ababa (Ethiopia), Atlanta (USA), Belfast (Northern Ireland), Buenos Aires (Argentina), Calgary (Canada), Can Tho (Vietnam), Cape Town (South Africa), Colima (Mexico), Greater Manchester (England), Greater Miami and the Beaches (USA), Guadalajara Metropolitan Area (Mexico), Haiyan (China), Honolulu (USA), Jaipur (India), Jakarta (Indonesia), Kyoto (Japan), Lagos (Nigeria), Louisville (USA), Luxor (Egypt), Melaka (Malaysia), Minneapolis (USA), Montevideo (Uruguay), Nairobi (Kenya), Nashville (USA), Panama City (Panama), Paynesville (Liberia), Pune (India), Salvador (Brazil), Seattle (USA), Seoul (Korea), Tbilisi (Georgia) Tel Aviv (Israel), The Hague (The Netherlands), Toronto (Canada), Vancouver (Canada), Washington, DC (USA), Yiwu (China). *Id.*

[90] *See* Michael Berkowitz, *What a Chief Resilience Officer Does*, 100 RESILIENT CITIES (Mar. 18, 2015), http://www.100resilientcities.org/blog/entry/what-is-a-chief-resilience-officer1#/-_/.

[91] *Id.*

privacy in the midst of the big data environment that results from making cities "resilient" in the face of change or disaster.[92]

II. Smart Cities and Privacy

Cities will often have no alternative but to collect personal or identifiable information if they are going to become "smarter." There may be some situations for which anonymous information may suffice. For example, data showing the volume of traffic may help guide decisions to reroute traffic to a less congested road. In Santander, for example, an intellectual property professional who works on the project said, "[w]e don't register the users. What we know is a user is using the application."[93] But there are other situations in which personal or identifiable information must be collected in order for the data to be useful. For example, law enforcement extensively uses license plate readers for a variety of security issues, including the tracking and apprehension of criminals.[94] But this data also presents many privacy concerns as it can potentially record and track the movements of every person driving by the license plate readers. This example illustrates the important balance between security (or some other important civic interest) and privacy that exists whenever personal information is collected.

Protecting privacy in the city of the future can be viewed in its historical context. Vint Cerf, Google's Chief Internet Evangelist and a "Founding Father of the Internet," believes that privacy is a relatively recent notion, "an artificial construct of the industrial age,"[95] that did not, and does not, exist in small towns.[96] Ironically, given the privacy-threatening trajectory of primarily urban smart cities, he describes the modern notion of privacy as a construct of the advent of the large urban center.[97] A 1973 report from the Department of Health, Education, and Welfare expresses a similar view—that there is much less privacy in a small town than in a big city.[98] The following example from Santander illustrates this point. A webmaster at the city's largest newspaper who does not use Facebook because of privacy concerns does not have a problem sharing data on the Santander apps because that is what cities are all about: "In Santander, everyone knows everyone."[99]

[92] *See infra* Part II.D.

[93] *See* Frayer, *supra* note 45.

[94] *See* Joh, *supra* note 81, at 48 n.87.

[95] Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 Fordham Urb. L.J. 1581, 1590 (2014).

[96] *Id.*

[97] *Id.* at 1590–91.

[98] *Id.* at 1591.

[99] Frayer, *supra* note 45.

Even if privacy is a relatively modern development born of the modern city, a "profound difference between privacy concerns of pre-industrial towns and those raised in hyperconnected cities lies in the power dynamics among stakeholders."[100] Though information shared by users may appear to travel in distinct vertical paths—whether it be traffic or parking or water-related—it goes to the same place: the government.[101] In addition, consumers have become desensitized in large part to practices that just a few short years ago would have been deemed "creepy."[102] In sum, "[t]he normalization of big data collection by city government increasingly raises the specter of a panoptic gaze."[103]

Legal discussion of smart cities is, however, a fairly recent development. A 2014 symposium devoted to the notion of building resilient cities included discussions about disaster response, deconstruction and reconstruction of cities,[104] economic planning for land use and urban growth, and planning issues regarding fire and water.[105] Further discussions focused on storm recovery after Hurricane Sandy[106] and bridging physical and human communities, as well as the social–ecological connection between these two systems.[107] Scholars proposed that an integrative

[100] Finch & Tene, *supra* note 95, at 1593 ("While traditional cultures and small villages saw information shared horizontally among citizens, the new urban landscape features a dramatic shift to vertical information sharing between citizens and government.").

[101] *Id.* at 1594.

[102] *Id.* at 1595.

[103] *Id.*

[104] *See* Stephen R. Miller, Symposium Introduction, *Resilient Cities: Environment | Economy | Equity*, 50 IDAHO L. REV. 1, 2–4 (2014). The call for papers included the following provocative definition by David Godschalk:

> A resilient city is a sustainable network of physical systems and human communities. Physical systems are the constructed and natural environmental components of the city. They include its built roads, buildings, infrastructure, communications, and energy facilities, as well as its waterways, soils, topography, geology, and other natural systems. In sum, the physical systems act as the body of the city, its bones, arteries, and muscles . . . . Human communities are the social and institutional components of the city. They include the formal and informal, stable and ad hoc human associations that operate in an urban area: schools, neighborhoods, agencies, organizations, enterprises, task forces, and the like. In sum, the communities act as the brain of the city, directing its activities, responding to its needs, and learning from its experience.

Id. at 2 (quoting David R. Godschalk, *Urban Hazard Mitigation: Creating Resilient Cities*, 4 NAT. HAZARDS REV. 136, 137 (2003)).

[105] The panel discussions at the 2014 Idaho Law Review Symposium included the following presentations: Introduction and Welcome; Disaster, Destruction, and Resilient Cities; Social Aspects of Resilient Cities; Resiliency, Equity, and Economy; and Resiliency and Planning for City Growth. *2014 University of Idaho Law Review Symposium*, 50 IDAHO L. REV. 1 (2014), http://www.uidaho.edu/law/law-review/symposium/2014-resilient-cities.

[106] *See* Andrea McArdle, *Storm Surges, Disaster Planning, and Vulnerable Populations at the Urban Periphery: Imagining a Resilient New York After Superstorm Sandy*, 50 IDAHO L. REV. 19 (2014).

[107] *See* Melissa M. Berry, *Thinking Like a City: Grounding Social-Ecological Resilience in an Urban Land Ethic*, 50 IDAHO L. REV. 117, 118–20 (2014). Berry argues that Godschalk's definition needs to be revised to "recognize the connection between the physical and the human systems . . . . The connection between those systems creates a new system: a social-ecological system." *Id.* at 126.

approach was probably the best way to discuss resilience, emphasizing the importance of the presence of an adaptable legal system.[108]

The proliferation of data collection and its aggregation in general society, coupled with the extensive data collection and integration of data in systems designed for a smart city, threatens fundamental individual privacy. Despite its benefits, big data in the smart city can open up the details of everyday life for analysis. Living in a panopticon,[109] where private lives become public—or at least perceived as public—is harmful to the very essence of privacy and the necessary freedoms that are important for autonomy and even democracy. Yet, balancing the public benefits of big data for creating resilient cities with the concomitant loss of individual privacy is difficult to do in "a legal environment which has yet to impose significant regulations on big data or the new 'Internet of Things' . . . ."[110] Therefore, principles of general privacy law must be used to analyze privacy protections. Privacy law is comprised of a complex system of statutes, constitutional law, administrative jurisdiction, and self-regulation. While it is beyond the scope of this Article to map this complex system of privacy protections, or perhaps more accurately a system of systems, two important components of privacy protection and regulation will be briefly examined: the U.S. Constitution and the Fair Information Privacy Practices ("FIPPs"). A smart city's collection and storage of personally identifiable information at a minimum implicates the Fourth Amendment reasonable expectation of privacy, and FIPPs have been widely used in an array of circumstances in order to protect individual privacy choices.

A. Weakness of Fourth Amendment Protections in the Smart City

Broadly viewed, smart city programs and privacy concerns are part of the age old debate about how, or if, law can respond to technological advances in an effective manner. Threats to privacy have often been seen in this light—from the Kodak camera to cookies on a hard drive to sensors in the bedroom.

Indeed the birth of the American right to privacy was fueled by an article written by Samuel Warren and Louis Brandeis in response to Kodak's introduction of the portable "snap camera."[111] Technology often drives not only changes in society, but also changes in the law. The U.S. Supreme Court is often the final arbiter of how society must deal with progress.

[108] Craig Anthony (Tony) Arnold, *Resilient Cities and Adaptive Law*, 50 Idaho L. Rev 245, 248 (2014).

[109] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1934–52 (2013) (discussing Jeremy Bentham's Panopticon, the description of a prison system where constant surveillance creates a panopticon and resulting control, George Orwell's Big Brother, and modern-day surveillance).

[110] *See* Finch & Tene, *supra* note 95, at 1607.

[111] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

In 1977, in *Whalen v. Roe*, the Supreme Court addressed for the first time what we would today call informational privacy.[112] The Court had to decide whether a state-mandated, centralized database containing prescription information of certain categories of controlled substances violated the privacy interests of those patients whose names were contained in the database.[113] In balancing the issues pertaining to the mainframe technology of the day, the Court concluded that the state's interest outweighed those of the individuals.[114] The Court recognized the growing "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[115] It stated that the "right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[116] Quite presciently, Justice Brennan stated in a concurring opinion that while he was satisfied with the safety measure employed by that system, he was "not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[117]

In 2001, in *Kyllo v. United States*, the Supreme Court held that the use of a thermal-imaging device that police aimed at a private home from a public street in order to detect relative amounts of heat contained within the home constituted a search under the Fourth Amendment.[118] There is a great deal of language from that decision that may be relevant to some of the privacy concerns of a smart city. The Court recognized that it "would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology" and that "[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[119]

The Court stated that while the device in question was relatively crude and could detect only visible light emanating from the home, "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[120] The Court refused to limit privacy protection in the home to only "intimate details," holding that any details of the home—even the details of how warm or relatively warm Kyllo kept his home—were privileged.[121] The Court noted that the device was

[112] Whalen v. Roe, 429 U.S. 589, 598 (1977).
[113] *Id.* at 592–95.
[114] *Id.* at 598–604.
[115] *Id.* at 605.
[116] *Id.*
[117] *Id.* at 607 (Brennan, J., concurring).
[118] Kyllo v. United States, 533 U.S. 27, 40 (2001).
[119] *Id.* at 33–34.
[120] *Id.* at 36.
[121] *Id.* at 38.

capable of disclosing, "for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system might detect nothing more intimate than the fact the someone left a closet light on."[122] The Court concluded by stating that while it may be true that there was "no 'significant' compromise of the homeowner's privacy" in this instance, the Court "must take the long view, from the original meaning of the Fourth Amendment forward."[123] In the smart city, government agencies or quasi-governmental service providers will have access to just that type of information; and even further, due to mobile devices, they will even know where in the house the homeowner sits.

Another decision relevant to the Fourth Amendment's potential application to big data and the smart city involved police installation of a GPS tracker on a car without a sufficient warrant to cover the one month surveillance.[124] The government argued that the car was in public view, and therefore the subject could have no expectation of privacy in its location.[125] By unanimous decision, yet with different rationales, the Supreme Court held that the constant and extended surveillance of the individual without an applicable warrant was a violation of the Fourth Amendment. A four justice concurring opinion applied a reasonable expectation of privacy test, stating that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[126] Writing for the concurrence, Justice Alito discussed the problems of an evolving expectation of privacy in the face of changing uses of technology.[127] Justice Sotomayor, in a concurring opinion, examined the challenge of digital surveillance in our high-tech society more broadly, contemplating that being subject to extensive data collection in everyday life should not mean that citizens must forfeit an expectation of privacy.[128]

Most recently, on March 30, 2015, the Supreme Court vacated, *per curium*, a lifetime GPS tracking order imposed on a North Carolina man who was convicted of taking indecent liberties with a child, and whose subsequent classification as a recidivist led to the continuous monitoring order.[129] Without an accompanying opinion, one may only infer that continuous monitoring invites constitutional scrutiny, and that this scrutiny may likewise be applied to the continuous data collection of potentially intimate details of everyday life in a smart city.

[122] *Id.*

[123] *Id.* at 40.

[124] United States v. Jones, 132 S. Ct. 945, 948–49 (2012).

[125] *Id.* at 948.

[126] *Id.* at 964 (Alito, J., concurring).

[127] *Id.*

[128] *Id.* at 955 (Sotomayor, J., concurring).

[129] Grady v. North Carolina, 135 S. Ct. 1368, 1371 (2015).

While these recent Supreme Court cases involve a specific police action and order by the justice system rather than public monitoring in general, the interests involved are closely tied. Surveillance in the smart city is constant, similar to the 24/7 surveillance that was found to violate the Fourth Amendment in *Jones* and *Grady*. The monitoring is likely to be without consent, and as described earlier, systems designed for city resilience can be as intrusive as monitoring the electricity use within a person's home or as public as tracking her movements in the city. Data from different surveillance systems can be aggregated, and much like the Internet of Things, the continual and prevalent use of sensors in a myriad of ways is neither regulated nor addressed by case law. While similar, the context of government surveillance for building smart cities is sufficiently different in that it is difficult to predict whether the recent line of Supreme Court rulings might be found applicable to limit the terms of surveillance in the not-too-distant future smart city. In contrast to the unclear application of Fourth Amendment jurisprudence to smart cities, the principles of behavior reflected in the FIPPs, which underlie many privacy laws and guide Federal Trade Commission actions, are clearly relevant. However, as discussed in the next Part of this Article, the implementation of these principles is at least problematic and arguably impossible.

B. Fair Information Practices: Theory and Failures

One of the most widely influential approaches to a system of privacy protection for individual information collection and use originated in a report issued by the Department of Health, Education and Welfare in 1973 addressing new issues pertaining to the computerization of health records.[130] This Code of Fair Information Practices has been the basis for much of the development of privacy and data protection. The basic principles enunciated in the report were as follow:

[130] *See* U.S. Dep't of Health, Educ. & Welfare, No. (OS)73-94, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973). For a thorough discussion of the history and evolution of fair information practices, see Robert Gellman, *Fair Information Practices: A Basic History*, http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf (last updated June 17, 2016); *see also* The White House, National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy 45 app.A (2011) ("FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.").

> (1) There must be no secret personal data record-keeping system.
>
> (2) There must be individual access to determine what information is collected and how it is used.
>
> (3) Use must be limited to the original purpose unless a person consents otherwise.
>
> (4) An individual must be able to correct or amend a record.
>
> (5) The record must be accurate, and reasonable steps must be taken to assure its appropriate use.[131]

In 1980, the Organisation for Economic Cooperation and Development ("OECD") expanded these basic principles and they have since become internationally recognized in various ways.[132] Greatly influenced by the OECD Guidelines, the European Union adopted the Directive on Data Protection ("Directive") in 1995.[133]

In 1998 the Federal Trade Commission ("FTC") identified "the five core principles of privacy" as: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress.[134] By 2000, the FTC condensed the five into "four widely-accepted fair information practices" for online information collection: notice, choice, access, and security.[135] Although definitions of the FIPPs are thus variable, we refer to these four FTC principles in further discussion.

FIPPs have become known as a notice and choice regime; individuals are entitled to be given notice of what information is collected and how it is to be used so that they can make an informed choice about whether to consent to its collection and use. Many websites have voluntarily adopted these principles,[136] and the FTC has exerted its section 5 authority over entities who do not follow the privacy practices

[131] *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 130, at xx–xxi.

[132] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Jan. 16, 2017). The principles include the following: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. *Id.*

[133] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC). *See* Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57, 59–61 (2000).

[134] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7–10 (1998).

[135] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE—A REPORT TO CONGRESS iii (2000).

[136] The Direct Marketing Association has the following statement regarding self-regulation on its website:

> Self-regulation is the most efficient and effective way to respond to privacy issues related to marketing and advertising. For this reason, when the Federal Trade Commission (FTC) raised concerns about the privacy implications of Interest-Based Advertising, DMA partnered with other large media and marketing associations to launch the Self-Regulatory Program for Interest-Based Advertising, which gives consumers a better understanding of and greater control over ads that are customized based on their online behavior (also called "interest-based" advertising).

Self-Regulation, THE DMA, http://thedma.org/accountability/self-regulation/ (last visited Jan. 16, 2017).

that they describe,[137] so that there is some means of enforcement. But difficulties with the FIPPs abound in the electronic, mobile, and social media environment, where true consumer choice is elusive and options, if any, are hidden in the privacy terms of websites or apps.[138] As noted in the 2014 report *Big Data and Privacy: A Technological Perspective*, prepared for the President, it is "only in some fantasy world" that individuals are able to read, negotiate, and meaningfully consent to privacy notices given by service providers.[139] The report describes the problem as a power differential, and the individual's *lack* of power as a market failure.[140] There is no reason to believe that the failed market for privacy will be any different in the "metropticon"[141] of the future.

The smart city of the future will not only feature surveillance by governmental entities, but will also likely embed and aggregate both public and private sector sensors and link the data produced to individuals. The fitness app worn by a citizen, and the GPS system in his or her car, may be integrated with public sensors that will warn the individual of impending traffic, inclement weather warnings, or some other event of "shock and awe." The noblest intent of the private and public interrelated systems is to protect citizens in the city and to warn and prepare them for disruptive events. However, considering the ubiquitous nature of information collection in the smart city, it is improbable that the individual will have meaningful notice of surveillance methods and of interrelated individual information collection and sharing. Likewise, it is unlikely that a meaningful choice will be available to each person who wishes to travel in and around that city. Similar to the demise of effective notice and choice mechanisms in the Internet of Things, even if a physical method of delivering notice and consent is designed, the constant monitoring and requests for consent will replicate the power imbalance and will lead to similar unsatisfactory results. Therefore, specific laws and regulations might be necessary for the smart city, data collection, and the preservation of individual privacy. Some localities have already taken action to address the concerns of their citizens.

[137] For case summaries of FTC actions against defendants such as Snapchat, Inc., TRUSTe, Inc., and Innovative Marketing, Inc., see FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE (2014).

[138] *See* Nancy J. King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 FED. COMM. L.J. 229, 255 (2008) (describing the notice and consent requirements for mobile advertising); Andrew Proia et al., *Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead*, 16 MINN. J. L., SCI. & TECH. 145, 199–200 (2015) (discussing the Internet of Things and problems for exercising consent).

[139] EXEC. OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (2014) ("Reality is different.").

[140] *Id.*

[141] *See* Finch & Tene, *supra* note 95, at 1581 (coining the term in the title of the article: "metropticon").

C. Approaches to Regulating Surveillance in the Smart City

Local laws already vary greatly as to the collection and retention of personal data from devices and sensors that are used in a smart city. New Hampshire at one point banned license plate reader use entirely,[142] but has since amended the law to provide for specific exceptions.[143] Some cities and states have mandated maximum retention periods for data from these devices, in time periods ranging from twenty-four hours to five years.[144] Others permit indefinite retention.[145] New Hampshire requires express permission before a smart grid device can be installed in a home.[146] Pending legislation in seven other states—Iowa, Massachusetts, New York, Rhode Island, Pennsylvania, Tennessee, and Michigan—would permit consumers to opt out of participation in the smart grid.[147] California, Colorado, and Oklahoma limit the ability of a utility company to sell or share smart grid data,[148] and other states are considering legislation that would protect this information.[149]

The Chicago AoT project has adopted a unique approach to protecting privacy by promising not to collect *any* personal or private information.[150] The "technology and policy have been designed to specifically minimize any potential collection of data about individuals, so privacy protection is built into the design of the sensors and into the operating policies."[151] Sound

[142] *See* N.H. Rev. Stat. Ann. § 261:75-b (2016).

[143] *See id.* § 236:130(III). Ten states now regulate usage of license plate readers to some extent by legislation and an additional two by virtue of Attorney General opinion or directive. *See Automated License Plate Readers: State Statutes Regulating Their Use*, Nat'l Conf. of State Legislatures (Apr. 13, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx; *see also* Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 Me. L. Rev. 397, 404–10 (2014).

[144] *See* Jessica Gutierrez Alm, *The Privacies of Life: Automatic License Plate Recognition Is Unconstitutional Under the Mosaic Theory of Fourth Amendmen* [sic] *Privacy Law*, 38 Hamline L. Rev. 127, 133–34 (2015) (listing a variety or retention periods from forty-eight hours to one year).

[145] *Id.* at 134 (stating that the New York State Police Department may keep its data indefinitely).

[146] N.H. Rev. Stat. Ann. § 374:62(II)(a) (West 2013). *See P*eppet, *supra* note 31, at 110–11.

[147] *See* Cassarah Brown, *States Get Smart: Encouraging and Regulating Smart Grid Technologies*, Nat'l Conf. of State Legislatures (July 2013), http://www.ncsl.org/research/energy/regulating-and-encouraging-smart-grid-technologies.aspx.

[148] *See* Peppet, *supra* note 31, at 111 n.164.

[149] Texas has already enacted such legislation and Tennessee is considering it. *See* Brown, *supra* note 147.

[150] *See* Array of Things, *supra* note 72.

[151] *Id.*

sensors will collect data on ambient volume, but "will neither record nor transmit the raw microphone data."[152] There will be a low-resolution camera in each node but "[a]ll images will be processed into numerical data within the node, after which image data will be immediately deleted. After initial calibration, no images or video will be stored within or transmitted from the video nodes."[153] In the initial plan, sensors were intended to detect Bluetooth and WiFi cell phone signals. While both types of information would be useful to achieve some of the project's goals regarding pedestrian and traffic patterns, concerns about the collection of identifying information caused the elimination of those sensors from the final plan.[154] According to the information on its website, none of the sensors collect personal or private information.[155] For future developments and decisions, "[a]ll hardware, software and data being collected will be regularly reviewed by a Technical Security and Privacy Group . . . . as an external, independent review team" and "the committee will also be consulted whenever there is a request for a new kind of data to be collected."[156]

Seattle's approach to smart city development is designed to use and manage personal information "in a manner that builds public trust."[157] "The City of Seattle Privacy Program" is designed to provide city employees guidance and tools to assist in incorporating the following actions into daily operations that involve personal information: minimizing data collection, providing notice, reviewing legal obligations,

> All hardware, software and data being collected will be regularly reviewed by a Technical Security and Privacy Group chaired by Von Welch, director of Indiana University's Center for Applied Cybersecurity Research. Operating as an external, independent review team, the committee will also be consulted whenever there is a request for a new kind of data to be collected. The Array of Things Executive Oversight Council will be co-chaired by Commissioner of the City's Department of Innovation and Technology Brenna Berman, Urban Center for Computation & Data Director Charlie Catlett, with additional members selected from academia, industry, non-profits, and the community. No data will be monitored without the approval of the privacy and security external oversight committee, the City of Chicago and the AoT executive committee, and the operation of the Array of Things will be governed by privacy policies that will be published prior to installation of nodes.

Id.

[152] *See FAQ*, *supra* note 74.

[153] *Id.*

[154] *See* Whet Moser, *Chicago's 'Array of Things' Takes Another Step Towards Reality*, CHI. MAG. (Sept. 17, 2015), http://www.chicagomag.com/city-life/September-2015/Chicagos-Array-of-Things-Takes-Another-Step-Towards-Reality/.

[155] *See FAQ*, *supra* note 74.

[156] *See* ARRAY OF THINGS, *supra* note 72.

[157] *Privacy*, SEATTLE INFO. TECH., http://www.seattle.gov/tech/initiatives/privacy (last visited Jan. 16, 2017); THE CITY OF SEATTLE PRIVACY PROGRAM: A PRINCIPLES-BASED APPROACH TO INCORPORATING PRIVACY PRACTICES INTO OUR DAILY OPERATIONS, CITY OF SEATTLE, http://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyProgramIntroductionE-TeamBriefing.pdf (last visited Jan. 16, 2017).

reviewing data, and systems security and deleting or de-identifying data according to our data retention schedules.[158]

"Seattle is leading the nation to implement a comprehensive privacy program across all City departments," according to Mayor Ed Murray.[159] "Our privacy principles are designed to protect individual privacy while still providing government transparency."[160] To further this aim, the city issued a privacy statement[161] based upon a set of previously proposed privacy principles.[162]

The Seattle Privacy Statement provides that it "applies to the collection, use, disclosure, sharing and retention of personal information [ ] obtain[ed] from individuals interacting with City departments, whether in person, on a website . . . or by mail in the course of providing City services."[163] The goal of the policy is "to collect only enough information as is reasonable to perform [ ] [s]ervices and to let you know when providing personal information is optional. We also seek to aggregate or otherwise de-identify personal data, when possible, whenever it is not necessary to store or share personally identifiable data elements."[164] The Statement provides that "[i]f you do nothing during your visit to our web site but browse, read pages, or download information, we will automatically gather and store certain information about your visit through the use of cookies and other similar tracking technologies. This information does not identify you personally."[165] Seattle has a three-step privacy review process for those who manage city projects and programs.[166] First, an agency must perform a Self-Service Assessment to determine what personal information is involved in the data collection, and, using Privacy Toolkit resources and an online questionnaire, decide whether further review is necessary.[167] If a need for further review is indicated, a Privacy Threshold Analysis is used to determine what further level of review is required.[168] Finally, if

[158] *Id.*

[159] Press Release, Office of the Mayor, Edward B. Murray, City Rolls out Innovative Privacy Program (Oct. 12, 2015), http://murray.seattle.gov/city-rolls-out-innovative-privacy-program/#sthash.ApWQIKHy.dpbs.

[160] *Id.*

[161] City of Seattle, City of Seattle Privacy Statement (2015), http://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/CityOfSeattlePrivacyStatementFINAL.pdf.

[162] Press Release, Office of the Mayor, Edward B. Murray, Seattle Poised to Be Leader in Protecting Resident Privacy (Feb. 3, 2015), http://murray.seattle.gov/seattle-poised-to-be-leader-in-protecting-resident-privacy/#sthash.S2pwJ3vX.dpbs (pledging to value citizen privacy, to limit collection, to be accountable, accurate, and transparent to the extent possible, and to follow state and federal laws regarding proper information disclosure).

[163] *See* City of Seattle, *supra* note 161, at 2.

[164] *Id.*

[165] *Id.* at 3.

[166] *Id.*

[167] *Id.* at 7.

[168] *Id.*

necessary, a Privacy Impact Assessment is completed, with assistance from a Privacy Champion and Privacy Program Manager, in order to identify privacy impacts and to plan for mitigation.[169]

Finding an appropriate balance between allowing for a city's collection of data in order to protect and promote citizens' health, while also protecting the personal privacy of its citizens, can be difficult. Libby Schaaf, the Mayor of Oakland, California, summarizes it well:

> It's really frustrating. On one hand we have an obligation to use tools that can save lives, can create safety, can prevent harm. And yet at the same time we have an obligation to respect and protect the privacy of the people who live here. . . . Help us not just say "hell no," to every form of technology that potentially could violate your privacy, but to help answer us the question: How, when, where and why? Because I think we have an obligation to figure out how to responsibly use these tools, and we have not done that.[170]

In the absence of clear legislative or judicial guidance about information gathering and privacy in the smart city, officials are placed in the position of navigating the gaps between technology and public policy. Self-regulation and ethical decisionmaking can help close that gap, at least in part.

D. Self-Regulation

Voluntary, self-regulatory methods of addressing privacy questions in the smart city include both ethical frameworks and technical approaches for incorporating privacy principles into smart city systems.

1. Ethics

Even beyond the smart city context, "[w]here once data was collected only for a specific purpose, now massive amounts of data are opportunistically and passively collected and reused in multiple contexts, over an indefinite time frame, often without informed consent."[171] Furthermore, with the use of predictive modeling, information about individuals can often be inferred from existing data. Importantly, "if ethics is not consciously considered at the inception of data projects, steps taken to increase community resilience could in fact create more vulnerability and thus do harm."[172]

Scholars propose that an ethical framework for data collection should enable individuals and communities to make informed decisions

[169] *Id.* at 10.

[170] Cyrus Farivar, *How One Mayor Struggles with Balancing Privacy and Surveillance*, ArsTechnica (May 25, 2015, 10:00 AM), http://arstechnica.com/tech-policy/2015/05/how-one-mayor-struggles-with-balancing-privacy-and-surveillance/.

[171] Kate Crawford et al., Big Data, Communities and Ethical Resilience: A Framework for Action 2 (2013).

[172] *Id.*

about how, where, why, and whether their data is to be used and for how long.[173] Furthermore, the responsibility for such a system should not be placed solely on individual users to read and understand complicated and obfuscated privacy policies. Rather, a data project management system should be adopted that promotes and builds trust and confidence among users in the ethical nature of the system.[174] Another part of an ethical data framework is big data due process, which would ensure fairness in the decisionmaking process.[175]

In 2013 the Rockefeller Foundation convened a select multidisciplinary group of fellows[176] to discuss smart cities' goal of big data and resilience.[177] The group proposed a draft "Code of Conduct" for community projects using big data[178] that was intended to create best practices that are "socially just, encourage local wealth- & skill-creation, require informed consent, and . . . [that are] maintainable over long timeframes."[179] While the draft details seven principles, two are of particular relevance here because they emphasize ethics, introducing a number of ethical concerns and recommending principles for conduct.[180] The broad principle of ethical data sharing has multiple aspects according to this group. Transparency is required for ethical data collection, as "communities should be able to see where their data goes, and a complete list of who has access to it and why."[181] Opt-in permission should be prioritized and individuals should be able to remove their data whenever they so desire. Although data should be shared, including with NGOs, academics, and humanitarian groups, careful negotiation of privacy protocols that distinguish between non-profit and commercial uses should be carefully negotiated. Profit-centered sharing should be adopted only when absolutely necessary and only if clear data protection policies exist to bind all subsequent data holders. The next principle related to ethics is the right to be free from government and private surveillance: "It is essential that the collection of any sensitive data, from social and mobile data to video and

[173] *Id.* Ethical considerations permit users to have "both granular control of data collection and retention, and the ability for users to opt out." *Id.* at 4.

[174] *Id.*

[175] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014).

[176] *See* Crawford et al., *supra* note 171, at 1.

[177] The program was cosponsored by an organization called PopTech. For a description of the meeting and thoughts of a participant, see Patrick Meier, *How to Create Resilience Through Big Data*, iRevolutions (Jan. 11, 2013), http://irevolution.net/2013/01/11/disaster-resilience-2-0/.

[178] *See* Kate Crawford et al., *Seven Principles for Big Data and Resilience Projects*, iRevolutions (Sept. 23, 2013), http://irevolution.net/2013/09/23/principles-for-big-data-and-resilience/.

[179] *Id.*

[180] *Id.* (providing that the remaining principles include using open source data tools, using transparent data infrastructure, developing and maintaining local data skills, adopting local data ownership, and learning from mistakes).

[181] *Id.*

photographic records of houses, streets and individuals, is done with full public knowledge, community discussion and the ability to opt out."[182] This principle speaks to "Data Philanthropy," a framework that gives individuals the power either to consent to being involved or to opt-out of participation in the smart city.[183]

Whether these aspirational principles will be followed when using big data in smart cities is yet to be determined. The differing public and private interests that are represented in the implementation of a smart city may or may not embrace these somewhat lofty goals. A pragmatic addition to a self-regulatory and ethically motivated approach is to embed privacy into the technical sensors, data collection, and management processes.

2. *Privacy Enhanced by Technology and Process*

Beginning in the 1990s, there have been attempts to focus more attention on designing technological systems that are better able to provide privacy protection. Some of the efforts are known as Privacy-Enhancing Technologies ("PETs").[184] A PET is a system of "measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of functionality of the information system."[185] One classification describes seven basic principles of privacy enhancing technology: (1) limitation in the collection of personal data; (2) identification/authentication/authorization; (3) standard techniques used for privacy protection; (4) pseudo-identity; (5) encryption; (6) biometrics; and (7) audit ability.[186]

In contrast, Privacy by Design ("PbD") is a major attempt to embed privacy-protection into the life cycle of information gathering systems and technology by means of a mindset and a process. The objective of PbD is to "ensur[e] privacy protection and gaining personal control over one's own information."[187] The premises forming the approach are that

[182] *Id.*

[183] *Id.*

[184] *See* H. van Rossum et al., Privacy-Enhancing Technologies: The Path to Anonymity (Ronald Hes & John Borking eds., rev. ed. 1998); Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents (G.W. van Blarkom et al. eds., 2003), http://www.andrewpatrick.ca/pisa/handbook/handbook.html [hereinafter Handbook of Privacy].

[185] *See* Handbook of Privacy, *supra* note 184, at 33.

[186] *Id.* at 37.

[187] Info. & Privacy Comm'r of Ontario, Privacy by Design 2 (rev. 2013), https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf; Ann Cavoukian, Privacy by Design: Strong Privacy Protection—Now, and Well into the Future 2 (2011) [hereinafter Strong Privacy Protection]. *See generally* Ann Cavoukian, The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices 1 (2011) [hereinafter 7 Foundational Principles] (providing readers with additional clarification about the seven foundational principles described in *Privacy by Design*). Cavoukian created the term and process in the 1990s. Strong Privacy Protection, *supra*, at 1. A history of privacy by design and implementation can be found in *Strong Privacy Protection*. For a discussion of how privacy by design would

respect for privacy should be the default, and that protecting privacy is not a zero-sum game, meaning protecting privacy does not ultimately result in another value, such as security, being harmed.[188] In fact, security is a part of privacy and is an integral part of PbD, a part of the design to be built into every product at the beginning.[189] Furthermore, as privacy is built into products from a proactive rather than reactive lens, fewer instances of privacy violations will need to be remediated.[190] Finally, PbD calls for transparency in information collection and for open systems.[191]

In an attempt to map privacy design strategies to (largely E.U.) legal requirements, Jaap-Henk Hoepman describes four data-oriented strategies and four process-oriented strategies.[192] Two of the data-oriented strategies are particularly relevant here: minimize and aggregate—collect as little personal information as possible and keep it at its highest level of aggregation for as long as possible.[193] Latanya Sweeney suggests a similar approach, a "Selective Revelation System," that can be used for "privacy-preserving surveillance."[194] She suggests that a system keep data at the highest level of aggregation until it is necessary to dig deeper into identifying information. She proposes five paired levels of "Investigation Status" and "Identifiability":

(1) Normal operation—Sufficiently anonymous
(2) Unusual activity—Sufficiently de-identified
(3) Suspicious activity—Identifiable
(4) Problem suspected—Readily identifiable
(5) Problem detected—Explicitly identified[195]

Such a system design could be used in a smart city for different situations.[196] For example, smart city technology could be used to monitor

apply to big data, see Anna Monreale et al., *Privacy-by-Design in Big Data Analytics and Social Mining*, 2014 EPJ DATA SCI. 10, http://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-014-0010-4; *see also* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1410–13 (2011) (noting both U.S. and E.U. policy preferences for privacy by design, distinctions from privacy enhancing technologies, problems in adoption, and suggestions for greater success).

[188] *See* 7 FOUNDATIONAL PRINCIPLES, *supra* note 187, at 3–5.

[189] *Id.*

[190] *Id.*

[191] *Id.*

[192] *See* Jaap-Henk Hoepman, *Privacy Design Strategies (Extended Abstract)*, *in* ICT SYSTEMS SECURITY AND PRIVACY PROTECTION, 29TH IFIP TC 11 INTERNATIONAL CONFERENCE 446–59 (Cuppens-Boulahia et al. eds., 2014).

[193] *Id.* at 452–55.

[194] Latanya Sweeney, *Privacy-Preserving Surveillance Using Selective Revelation* 20 (Sch. of Comput. Sci., Carnegie Mellon U., Working Paper No. 15, 2005).

[195] *Id.*

[196] The European Union instituted a program for smart metering without considering the privacy implications. For a description of how Great Britain tried to adopt privacy later in the process rather than privacy by design at the outset, see Ian Brown, *Britain's Smart Meter Programme: A Case Study in Privacy by Design*, 28 INT'L REV. L. COMPUTERS & TECH. 172, 180 (2014) ("The most significant gap

health information in a school system. During normal operation, there would be no personally identifiable information revealed at all. If there is unusual activity, an increase of absenteeism, for example, more information would be made available at a school wide level. If the incidence of absenteeism increases further or appears to be very localized, additional information could be made available in order to address public health issues. Similarly, a citywide security system may monitor behavior at a macro level, and only when there is suspicious activity or a specific event would more identifying personal information be revealed. Obviously, there would need to be trust in such a system and verification that the procedures are operational, and are, in fact, used.

The vision of a smart city demands individually identifiable information, so laws that eliminate sensors that collect personal information may be only a temporary—or isolated—solution. For example, virtually any system that provides for security or healthcare would need to identify an individual at some point in time. Can laws or self-regulatory steps protect privacy in this environment? What is the most enduring approach? And most important, how can a city design a system that will ensure that privacy will survive in the face of disruptions by smart technology, surveillance, and data collection? The discussion that follows proposes that resilience theory can be used as a methodology to understand what is happening to privacy in the smart city, and furthermore can be used as a framework for comparisons and evaluation of approaches.

III. Resilience Theory and Privacy in the Smart City

Researchers have studied resilience, or lack of resilience, in differing contexts. For example, the ability of some species to survive catastrophic ecosystem changes while others become extinct, the ability of communities to overcome tragic events rather than fall apart and disperse, and the ability of individuals to thrive despite poverty rather than falling further into the cycle.[197] In the smart city, the collection of an immense amount of personal information aggregated for different uses threatens the core of personal privacy. Resilience theories can provide some understanding of whether different regulatory approaches might support the resilience of privacy or, alternatively, might be factors leading to its demise.

Interestingly, the word "resilience" finds its earliest roots in legal vocabulary. In the 1600s the term was included in a law dictionary, and its definition carried a negative connotation of failing to keep one's word,

between privacy by design principles and the design of Britain's smart metering programme was the lateness of serious consideration of privacy issues in the process.").

[197] *See* K. Sapountzaki, *Social Resilience to Environmental Risks: A Mechanism of Vulnerability Transfer?* 18 Mgmt. Envtl. Quality: Int'l J. 274, 277 (2007).

or to go back upon one's promise.[198] Over time, its association with bouncing back from a negative event became solidified, and the concepts of flexibility and recovery were added to the general use and understanding of the word.[199] In contrast, the law kept using it in a negative way, evolving to mean a breach of contract, and adding an element of fickleness to the meaning.[200] In sum, "resilience (*resiliency*, *resile)* has a long history of multiple, interconnected meanings in art, literature, law, science and engineering."[201]

The modern, general definition of the term resilience is "the capacity of a system to absorb disturbance and still retain its basic structure and function."[202] Though long in use, the term resilience began its modern analytical application in the discipline of ecology, particularly in the work of C. S. Holling in the 1960s and 1970s.[203] The concept is commonly applied in reference to the ability of a specific, natural ecosystem to survive, related to biodiversity, climate change, coastal systems, endangered species, offshore oil and gas, or watersheds.[204] Resilience is also discussed in diverse disciplines, such as structural engineering,[205] supply chain management,[206] social systems,[207] and urban planning.[208] In legal literature, "sustainability" is sometimes used as a

[198] *See* D. E. Alexander, *Resilience and Disaster Risk Reduction: An Etymological Journey*, 13 NAT. HAZARDS & EARTH SYS. SCI. 2707, 2709 (2013) ("The first known dictionary definition of resilience comes from the *Glossographia* compiled by the lawyer and antiquarian Thomas Blount." (internal citation omitted)).

[199] *Id.*

[200] *Id.*

[201] *Id.* at 2710.

[202] Tracy-Lynn Humby, *Law and Resilience: Mapping the Literature*, 4 SEATTLE J. ENVTL. L. 85, 89–90 (2014) (quoting BRIAN WALKER & DAVID SALT, RESILIENCE THINKING: SUSTAINING ECOSYSTEMS AND PEOPLE IN A CHANGING WORLD iii (2006)); *see* Arnold, *supra* note 107, at 245 ("Resilience is the capacity of a system to withstand or adapt to disturbance while maintaining the same basic structures and functions."). Arnold describes a resilient system as one that "has a high level of adaptive capacity. . . . [or] has enough flexibility, redundancy, and learning capacity to adapt to disturbances and surprises without collapse . . . ." *Id.* at 246. Arnold believes that this concept of resilience is largely replacing the concept of sustainability as a policy goal, in part because resilience is better able to be empirically observed. *Id.*

[203] *See, e.g.*, Holling, *supra* note 15; *see also* Carl Folke, *Resilience: The Emergence of a Perspective for Social-Ecological Systems Analyses*, 16 GLOBAL ENVTL. CHANGE 253, 254 (2006) (describing the "roots of the resilience perspective").

[204] *See* Humby, *supra* note 202, at 100 tbl.1; Li Xu et al., *Resilience Thinking: A Renewed System Approach for Sustainability Science*, 10 SUSTAINABILITY SCI. 123, 125 (2015) (comparing resilience definitions from various disciplines).

[205] *See* Haigh & Amaratunga, *supra* note 19.

[206] *See* Kirstin Scholten et al., *Mitigation Processes—Antecedents for Building Supply Chain Resilience Capabilities*, 19 SUPPLY CHAIN MGMT.: INT'L J. 211 (2014) (integrating disaster resilience practices with supply chain implementation).

[207] *See* W. Neil Adger, *Social and Ecological Resilience: Are They Related?* 24 PROGRESS HUM. GEOGRAPHY 347 (2000).

[208] *See* Henrik Ernstson et al., Report, *Urban Transitions: On Urban Resilience and Human-Dominated Ecosystems*, 39 AMBIO 531 (2010).

concept similar to resilience, although the use of the latter term seems to be increasing.[209]

The following Subparts explore three specific theoretical approaches to resilience—engineering, ecology, and socio-ecological—and then apply these concepts to privacy in a smart city. By viewing privacy and its protection through these theories, insights are sought for imbuing privacy with resilience, so that it might survive the threats to its existence in the smart city.

A. ENGINEERING SAFETY AND RESILIENCE ENGINEERING

Engineering safety is a precursor, so to speak, of resilience engineering. Safety engineering is the creation or design of systems in order to avoid unacceptable levels of risk, and the study of "why things go wrong."[210] In comparison, engineering resilience is defined as "[t]he intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions."[211] Four essential factors that contribute to a system's resilience are its ability to (1) respond to actual occurrences; (2) monitor ongoing threats; (3) anticipate potential disruptive events; and (4) learn from experience.[212] Overall, engineering resilience focuses on maintaining stasis equilibrium.[213] Following a disturbance, a resilient system would return to the equilibrium point relatively quickly,[214] and it is implied that the system would not vary greatly from the equilibrium point.[215]

Engineering resilience can apply to the resilience of a physical building perspective, for example. A building will experience extreme stress from the natural environment, such as from hurricanes or tornadoes. It must withstand those forces and maintain its fundamental structure as an edifice in order to be categorized as resilient. Architects and designers seek to build in features that will fortify the building's resilience from these elements.[216] If the integrity of the building is destroyed, the shell could be condemned, and it would lose its identity as a functioning building.

[209] *See* Humby, *supra* note 202, at 86–87; *see also* DAVID D. WOODS, RESILIENCE ENGINEERING: CONCEPTS AND PRECEPTS 1–6 (Erik Hollnagel et al. eds., 2006).

[210] *See* JEAN PARIÈS & JOHN WREATHALL, RESILIENCE ENGINEERING IN PRACTICE: A GUIDEBOOK xxix (Erik Hollnagel et al. eds., 2006) (describing safety engineering focus on avoiding unacceptable risk).

[211] *Id.* at xxxvi.

[212] *Id.* at xxxvii. The four cornerstones of resilience are responding, monitoring, anticipating, and learning. *Id.*

[213] *See* Fridolin Simon Brand & Kurt Jax, *Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object*, 12 ECOLOGY & SOC'Y 23, 23–24 (2007).

[214] *See* Philippe Bourbeau, *Resiliencism: Premises and Promises in Securitisation Research*, 1 RESILIENCE 3, 8 (2013).

[215] *See* Holling, *supra* note 13, at 33.

[216] *See* Haigh & Amaratunga, *supra* note 19, at 16.

To apply engineering resilience to privacy in the smart city, one must identify the point beyond which privacy ceases to be a viable concept and is, metaphorically speaking, condemned like the destroyed building. To preserve privacy, the city would then ban the activity that would destroy that essence of privacy, but allow for actions that might buffer but not destroy privacy. For example, if a person's location is always known in a smart city, and their use of resources is tracked, monitored, and adjusted, it might be said that they no longer retain a functioning right of privacy because of the intensity of the surveillance. Chicago's AoT project adopted an approach, at least in part, that can be categorized as an engineering approach as it has, in essence (1) identified privacy as the absence of personal surveillance, and (2) banned the collection of personally identifiable information in all of the embedded sensors or videos in the city,[217] so as to preserve that privacy. Initial plans for the AoT project included Bluetooth sensors, but privacy concerns voiced by citizens contributed to their elimination.[218]

FIPPs may also be categorized as an engineering approach to privacy because the elements of FIPPs—including transparency, control, and choice over the collection and use of personal information—create narrow boundaries.[219] Furthermore, notice and choice creates the equilibrium state for fairness and privacy; when a person is given notice and a choice about the use of their information, then the equilibrium is met. But this is a rigid system for defining what to protect to preserve privacy, and how to protect it. It allows for little flexibility for responding to change.

Engineering resilience holds that a system will bounce back and return in close proximity to a previous threshold. Assuming a point in time when an individual had control over the collection of his or her information, then under this view, in order for privacy to be resilient in a smart city, individuals would need to regain control over personal information in close approximation to what previously existed. Yet, the core principles of notice and choice are virtually impossible to implement in a sensor-embedded smart city.[220] Inflexibility and failure to adapt by

[217] *See supra* Part II.C.

[218] *See* Moser, *supra* note 154; Jolie Lee, *Big Brother? Chicago to Measure Pedestrians' Movements*, USA Today (June 24, 2014, 8:58 AM), http://www.usatoday.com/story/news/nation-now/2014/06/24/chicago-big-data-sensors/11301333/; Mike Wheatley, *Chicago Gets a Friendly Big Brother with the Array of Things*, siliconANGLE (June 23, 2014), http://siliconangle.com/blog/2014/06/23/chicago-gets-a-friendly-big-brother-with-the-array-of-things/.

[219] *See supra* Part II.B.

[220] *See generally* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1880–81 (2013) (discussing the failure of the consent paradigm due to lack of control and structural problems). Others would likely disagree. Julie Brill, a Commissioner of the Federal Trade Commission, believes that the key to the Internet of Things and user privacy is building trust and maximizing benefits through consumer control. *See* Julie Brill, Essay, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 Fordham L. Rev. 205, 214 (2014). Brill offers three best practices for device and service providers. First, because most of the

insisting on using the same FIPPs that have been used for decades could actually mean that privacy in the smart city will become extinct.

Engineering resilience and the laws and regulations that adopt this approach are too limited for the dynamic and rapidly changing environment of big data and smart cities. Ecological resilience takes a more flexible approach.

B. Ecological Resilience

The ecological concept of resilience originally resembled engineering resilience because it included the ability of a resilient system to maintain its fundamental attributes despite a disruption, bending without breaking and returning to its original state.[221] Later researchers modified the ecological concept, describing resilience as the ability to *absorb* attacks and *accommodate* greater deviations from the starting point without requiring the system to return to the *exact* central point.[222] Ecologically there was a shift in thinking, away from trying to count and maintain a certain number of a species in an environment toward trying to understand how species respond to a changing environment and how *relationships* between populations are maintained.[223] In brief, the results described the survival of ecological systems by adaptation into several different states of being. But while systems or organisms changed attributes they still retained the essential elements that described their identity.[224] As a result, in the environmental sense a resilient system is one that can "absorb changes . . . and still persist."[225] In addition, ecological resilience reflects how systems adapt to and manage external pressures,[226] and the maintenance of dynamic multistates of ecological existence.[227]

devices that make up the Internet of Things do not have user interfaces or easily accessible privacy policies, organizations need to build privacy and ethical considerations into their products. Brill is optimistic that more and more technologists will be trained in the ethical collection and use of data. The second best practice is the de-identification of data. Brill believes that companies need to "strip their data of identifying markers; . . . make a public commitment not to try to reidentify the data; and . . . contractually prohibit downstream recipients of the deidentified data from reidentifying it." *Id.* The third best practice is more effective transparency. Brill believes that there is a need for "shorter, clearer, and more standardized [consumer] notices" to make it easier to understand what information is being collected and transmitted by these new devices. *Id.* at 214–15.

[221] *See* Holling, *supra* note 13, at 33–34.

[222] *Id.* at 33.

[223] *See* Holling, *supra* note 15, at 14 ("But there is another property, termed resilience, that is a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables.").

[224] *See* Sapountzaki, *supra* note 197, at 275.

[225] *Id.* (describing progression of work of resilience scholars); *see* Lia Helena Monteiro de Lima Demange, *The Principle of Resilience*, 30 PACE ENVTL. L. REV. 695, 700 (2013).

[226] *See* Sapountzaki, *supra* note 197, at 275.

[227] *See* Brian Walker et al., *Resilience, Adaptability and Transformability in Social-Ecological Systems*, 9 ECOLOGY & SOC'Y 5, 7–9 (2004).

The ecological perspective of resilience requires that we consider the existence of different states of privacy, accepting that these states may change due to the proliferation of data and surveillance. Yet under the ecological theory of resilience, privacy will survive if it continues to reflect its fundamental meaning. In a super data-driven smart city, different thresholds of privacy may be identified in which some levels of surveillance are acceptable while others are not. Ecological resilience would not expect that the same privacy attributes exist in all aspects in the smart city. For example, a parking pass sensor at a parking garage will diminish a person's privacy, but it may not destroy fundamental privacy if the system requires that the data is kept secure and not shared beyond its use for parking purposes. A person's privacy will change after the installation of the parking pass, but its fundamental nature will persist in spite of the change.

The Supreme Court has recognized that privacy does not mean the same thing as it did before a camera could capture a person's image, a GPS tracking device could follow someone remotely every day of his or her life, or a thermal imaging device could capture intimate personal activities.[228] The Court's debates have recognized that privacy expectations are changing with the technology, yet they still focus on the limits in order to preserve the essence of what personal privacy entails. The evolution of concepts of privacy in response to advances in technology can be characterized as similar to an ecological resilience approach.[229] The Constitution and its arbiter, the Supreme Court, provide essential pillars for privacy resilience in the smart city by applying enduring values that transcend time, yet adapt to changing circumstances. The Fourth Amendment could potentially protect individual privacy in a smart city if jurisprudence develops in a way that recent cases might foreshadow. There is a problem, however. The Supreme Court will react only to a case or controversy and is constrained by the questions presented to it. Therefore, from the ecological resilience perspective, the Supreme Court has an essential yet narrow role to play in the adaptation of privacy in the smart city. The Court alone cannot provide the conditions for privacy resilience.

In some respects, PETs could be part of an ecological approach to privacy resilience. While a limited vision of PETs is that they are a means to enforce the same information practices as FIPPs, thus supporting an engineering resilience tactic of preserving the status quo, a broader vision of PETs can expand the options available under changing circumstances. Selective disclosure technology is in the category of an

[228] *See supra* Part II.A.

[229] *See* J.B. Ruhl, *General Design Principles for Resilience and Adaptive Capacity in Legal Systems—With Applications to Climate Change Adaptation*, 89 N.C. L. REV. 1373, 1379–80 (2011) (describing the U.S. Constitution as closely related to an engineering resilience strategy).

ecological approach because it recognizes that privacy preservation can be more nuanced than FIPPs and that there can be different levels of privacy based on the context and contributing factors.[230]

PETs do not, however, lead to discussion and development of an understanding about societal expectations for privacy, and constitutional review is limited to a specific controversy. Socio-ecological resilience theory, however, depends on a conversation about the meaning and essence of privacy in wider contexts of society.

C. Socio-Ecological Resilience

A third resilience theory is the socio-ecological approach. The coalescence of this theory is generally attributed to a paper published in 2000,[231] which proposed that ecological resilience principles could apply to social resilience when broadly defined.[232] Debate around the differences and codependency between social and ecological resilience is rigorous, and theories related to the resilience of socio-ecological systems are disparate.[233] In short, as humans and their institutions interact with or seek to manage nature, they intimately affect that environment and cannot be separated from it.[234] For example, in forest management, as policies and actions decrease the incidence of forest fires, forest undergrowth increases, thereby actually exacerbating the intensity of future fires.[235] Thus, one must consider not only the ecology of forests, but also the human policies and decisions that act upon them. Therefore, the baseline inquiry in a socio-ecological context is most likely to start with a discussion of whether resilience is a positive goal to be pursued.

Initially, the disruptive event must be identified through discourse as a negative occurrence, because it is "not by definition problematic or negative," but rather, it requires "[r]hetoric and discursive powers . . . to portray the event as a significant threat . . . ."[236] In the previous example, discussions would need to occur to decide whether forest fires are indeed negative events. In addition to this deliberative and normative foundation,

[230] *See supra* Part II.D.

[231] *See* Katrina Brown, Katrina Brown, *Global Environmental Change I: A Social Turn for Resilience?*, 38 Progress Hum. Geography 107, 110–11 (2014) (discussing a paper by W. Neil Adger).

[232] *See* Adger, *supra* note 207, at 347–48.

[233] *See* Michael Fabinyi et al., *Social-Ecological Systems, Social Diversity, and Power: Insights from Anthropology and Political Ecology*, 19 Ecology & Soc'y 28, 29 (2014). For a summary of criticisms of applying resilience theory to social systems, see Humby, *supra* note 202, at 94–95.

[234] *See* Humby, *supra* note 202, at 91.

[235] *See* Demange, *supra* note 225, at 702.

[236] *See* Bourbeau, *supra* note 214, at 13; *see also* Andrea M. Keessen et al., *The Concept of Resilience from a Normative Perspective: Examples from Dutch Adaptation Strategies*, 18 Ecology & Soc'y 45, 46 (2013) ("Using the concept of resilience in a social context therefore requires answering tough questions about the direction that adaptation should take. What society do we want to preserve or to reorganize into?").

the system's capacity for adaptation is an essential part of the socio-technical view of what resilience means. Adaptive capacity is considered to be "an iterative process of management that assumes that all knowledge is provisional and engages in a series of experiments that have feedback loops consisting of continuous monitoring, learning, and changes to management actions based on the lessons learned."[237] Different responses are possible as a result of the adaptive process. The system can evolve gradually and change incrementally due to the feedback loop and continuous learning, or it can resist change based on the necessity to maintain its identity.[238] Even if resistance is the course, the status quo is not necessarily inevitable, as this approach "rejects the idea that a single stable state sustains a system; even if well-functioning systems maintain their core characteristics, they will adapt to changing conditions and disturbances and undergo some degree of change from time to time."[239] Change can occur in reaction to the unsustainable effects of social policies, and transformation or renewal may happen as a result.[240]

A socio-ecological resilience approach to the smart city privacy domain requires public discourse as the first step. A conversation should examine whether preservation of privacy is a desirable state of being. Privacy protection could result in negative effects such as insecurity, lessened personalization, or the inability to conserve limited resources. In the smart city, protecting privacy might prevent the collection of personal data and thereby thwart disaster planning and fine-grained management of city resources. But the discourse must also include an examination of the inevitable impact that city collection of data about, and surveillance of, citizens can have on individuals and their relationships. A great irony is that when cities adopt intense surveillance and data-driven decisionmaking in order to efficiently and effectively interact with and manage citizens and their unique uses of resources, then they can discourage, rather than encourage, deliberative citizen engagement.[241] If a citizen's actions are always known, and thoughts and beliefs can be inferred, then there is less reason for government and citizens to interact in discursive ways.

In part PbD is a socio-ecological approach because it focuses on ways of thinking about relationships between privacy and other values such as security, and it rejects the notion that one necessarily excludes the other. PbD however adopts the FIPPs as its foundation without a

[237] Arnold, *supra* note 107, at 261.

[238] *See* Ruhl, *supra* note 229, at 1387–88.

[239] *See* Arnold, *supra* note 107, at 247.

[240] *See* Humby, *supra* note 202, at 94.

[241] *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV L. REV. 1904, 1912–18 (2013). "Privacy is one of the resources that situated subjects require to flourish." *Id.* at 1911.

view toward social adaptation and innovation, as well as technical innovation.

Seattle's approach to privacy is both iterative and evolutionary. When it launched its Privacy Initiative in September 2014, it recognized that there would need to be input and feedback from a variety of people and that it would be a long-term project.[242] The Privacy Principles, first of three deliverables, were adopted in February 2015.[243] The Privacy Policy[244] was accepted in July 2015 and the Privacy Statement[245] was approved in September 2015. In anticipation of modification over time, the latter two documents are both designated as "Version 1.0" and the Privacy Statement contains a "Document Control" section. There is an external Privacy Advisory Committee comprised of privacy researchers, practitioners, and community representatives.[246] The process is transparent, with a website containing recordings of all of the public meetings and translations of relevant documents in seven languages.[247]

Programs like that in Seattle demonstrate the dynamic interplay between the smart city and evolving meanings of privacy. They reflect a socio-ecological approach to understanding and building resilience. Instead of a choice between two polar opposites that is forced by using an engineering approach—privacy or the complete absence of privacy—legal and regulatory adaptation and innovation can respond to both of these environments and address change in a socio-ecological framework.

D. Summary

A comparison of three approaches to resilience shows that each one focuses on the survival of a system in the face of a disruptive event or change in the environment. All of the approaches also incorporate a systems viewpoint.[248] But each also possesses a unique perspective and organizing principles. The engineering approach focuses on a return to the original state of being, minimal fluctuations from equilibrium, and an emphasis on understanding system design and operation in order to increase successes rather than decrease failures. While the approaches share a focus on the ability to adapt and learn from severe events, the ecological differs from the engineering because it accepts wider

[242] *See Privacy*, *supra* note 157.

[243] *See id.*

[244] *See* City of Seattle, Privacy Policy (July 21, 2015) http://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyPolicyFINAL.pdf.

[245] *See* City of Seattle, *supra* note 161.

[246] *See Privacy Advisory Committee*, Seattle Info. Tech. (2015) http://www.seattle.gov/tech/initiatives/privacy/privacy-advisory-committee (last visited Jan. 16, 2017).

[247] *See Privacy*, *supra* note 157.

[248] *See* Brown, *supra* note 231, at 109–10.

variability from a norm and accepts that there may be different resulting states of being. In comparison, although the socio-ecological approach is derivative, in part from the ecological view of resilience, its focus on discourse, meaning, and resistance is what sets it apart.[249]

It is the argument of this Article that building engineering resilience for privacy is by itself insufficient to preserve the essence of the right to privacy caused by the disruptions of huge volumes of data collected and used in the smart city. Engineering resilience provides a necessary systems framework, and it requires clearly defined definitions of the privacy values to be protected. It does not recognize, however, that there can be different conceptions of privacy, and it would seek to preserve the status quo, as per FIPPs. Ecological resilience is a useful framework for privacy because it emphasizes the ability of a system to absorb changes rather than repel them, and it recognizes that there can be different states of privacy. The socio-ecological theory of resilience is important for the survivability of privacy because amidst swift and often opaque technical advances, society and citizens must address their choices and what privacy means in the smart city.

Keeping these important elements of each resilience framework in mind, the next Part examines the National Institute for Standards and Technology Privacy Engineering project as an example of the most recent effort to build privacy resilience.

IV. Building Privacy Resilience for the Smart City

The process of building resilience for privacy in the smart city can be modeled after the process and efforts to build a resilient critical infrastructure in cyberspace. In 2013, President Obama issued Executive Order 13,636—"Improving Critical Infrastructure Cybersecurity"[250]—which ordered the National Institute for Standards and Technology ("NIST") to develop a voluntary framework to secure critical infrastructures. While recognizing the potential negative impact on privacy, the Executive Order also required the NIST to consider the affect of cyber security recommendations on civil rights, including privacy.[251]

After engaging stakeholders across areas of interest, the NIST published a Cybersecurity Framework in February 2014 which lays out a risk-based adaptive process incorporating a learning feedback loop to

[249] There is no intent to diminish the complexity of the theories of resilience and the "panarchy" of interrelated systems by this general description of the three approaches to resilience. *See, e.g.*, J. B. Ruhl, *Panarchy and the Law*, 17 Ecology & Soc'y 31, 33 (2012) ("Panarchy [theory] leans heavily on the theory of complex adaptive systems, i.e., the study of systems comprising a macroscopic, heterogeneous set of autonomous agents interacting and adapting in response to one another and to external environment inputs." (emphasis in original omitted)).

[250] Exec. Order No. 13,636 78 Fed. Reg. 11,739 (Feb. 12, 2013).

[251] *Id.*

build resilience for cyber infrastructure. Yet the Framework noted that "additional best practices may need to be developed."[252] Subsequently, the NIST produced another document, the Privacy Risk Management ("PRM") for Federal Information Systems, to be used by system designers and operators and to provide a method for determining and addressing the risks to privacy within cyber infrastructure protection.[253] The NIST is also involved in promoting standards for smart cities, therefore the comparison of a resilient cyber infrastructure becomes relevant to the discussion of privacy in the smart city.[254]

A. NIST Privacy Framework

The PRM creates three engineering objectives to be implemented by system designers and operators in order to protect privacy: predictability, manageability, and dissasociability.[255] Predictability is the use of information in ways that are within the parameters that an individual would anticipate.[256] The objective is important because it develops trust between the data collector/system operator and the individual, thereby facilitating the self-determination.[257] Although transparency aids predictability, it is not equivalent, and neither knowledge about the details and methods of data collection nor the limitation of use or purposes are necessary to achieve predictability.[258] Thus, predictability implies that context is relevant for defining the parameters of privacy. Furthermore, the PRM contends that

[252] Michael Garcia et al., National Institute of Standards & Technology Internal Report 8062: Framework for Improving Critical Infrastructure Cybersecurity 15 (2014).

[253] Nat'l Inst. of Standards & Tech., Privacy Risk Management for Federal Information Systems (Sean Brooks & Ellen Nadeau eds., 2015).

[254] *See* Brian Kennedy, *NIST Tackles Cybersecurity in the Smart City*, Hogan Lovells Chron. of Data Protection (June 22, 2015), https://www.hoganlovells.com/en/blogs/hldataprotection/nist-tackles-cybersecurity-in-the-smart-city.

[255] *See* Garcia et al., *supra* note 253, at 18.

[256] *Id.* ("A reliable belief about what is occurring with personal information in a system."). The NIST's definition of predictability is as follows: "Predictability is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system." *Id.*

[257] *Id.* The Framework does not explain how it furthers self-determination, even though it does not implement user control.

[258] *Id.* at 18–19. The Privacy Framework seems to revise the definition of use and purpose in the FIPPs, and to minimize the importance of user control, by stating:

> Finally, predictability supports the translation or implementation of the FIPPs for use limitation and purpose specification in a manner that allows for innovation. For example, inherent in the rationale for use limitation is the recognition that changes in processing of personal information are loci for privacy risk. By focusing on maintaining reliable assumptions about that processing, predictability enables operators to assess the impact of any changes and target the application of appropriate controls. Thus, predictability facilitates the maintenance of stable, trusted relationships between information systems and individuals and the capability for individuals' self-determination, while enabling operators to continue to innovate and provide better services.

Id. at 19.

ex post control of unpredictable uses or outcomes is an alternative method for meeting the predictability objective.[259]

The predictability objective is more flexible[260] than a notice and choice regime. Seen through the lens of resilience theory, predictability has adaptive capacity and can respond to the circumstances.[261] Its application to data collection in smart cities would not prevent pervasive surveillance and big data applications. The NIST Framework maintains that new and innovative[262] collection of data may be undertaken even if individuals do not understand how technology is processing their information.[263] Therefore, smart city applications that combine information from the Internet of Things or share information across functional areas could be undertaken under the Framework. However, since predictability requires system operators to mitigate the system impact on privacy by implementing controls, smart city system operators might, for example, implement de-identification or restricted operator access to the data in order to preserve predictability.[264]

The manageability objective also does not implement user control of information use.[265] On the contrary, it refers to the *operator's* ability to maintain the required technical control of the system in order to achieve "accuracy and fair treatment of individuals,"[266] which could be adversely affected by inaccuracy and obsoleteness, and which is also required to implement elements of FIPPs.[267] In fact, the individual ability to control information is described as *harmful* for the functioning of some systems, such as identity management systems.[268]

Disassociability, which is broader than unauthorized access, envisions that system operators will protect individual information from "unnecessary exposure."[269] Cryptography is cited as a relevant technology that can promote disassociability. The NIST anticipates further work toward

[259] *Id.*

[260] *Id.*

[261] Adaptation as an essential part of resilience is discussed *supra* in Part III.C.

[262] *See* Garcia et al., *supra* note 253, at 19.

[263] *Id.* at 18.

[264] *Id.* at 19.

[265] *Id.*

[266] *Id.* at 20. The NIST defines manageability further as follows: "Manageability is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure." *Id.* at 18.

[267] *Id.* at 19 ("[M]aintaining data quality and integrity, achieving data minimization, and implementing individuals' privacy preferences.").

[268] *Id.* at 19–20.

[269] *Id.* at 20. The NIST defines disassociability further as follows: "Disassociability is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system." *Id.* at 18.

understanding how specific concepts such as anonymity or de-identification apply to disassociability.[270]

B. Privacy Risk Model

In addition to engineering objectives, the NIST proposed a Privacy Risk Model to conceptualize and gauge the potential individual harm to privacy caused by an information system.[271] The Privacy Risk Model by the NIST calculates the privacy risk to an organization as the "[l]ikelihood of a problematic data action" for individuals multiplied by the severity of its impact on the organization.[272]

Problematic data actions that will negatively impact privacy include: appropriation of personal information, distortion by inaccurate or incomplete information, induced disclosure of information, insecurity of the information, disproportionate surveillance, unanticipated revelation, and unwarranted restriction.[273] These problematic data actions can lead to privacy problems for individuals, which are categorized as: (1) loss of self determination, which includes loss of autonomy, exclusion, loss of liberty, and physical harm; (2) discrimination, which includes stigmatization and power imbalance; (3) loss of trust; and (4) economic loss.[274]

Interestingly, although problematic data actions and their subsequent privacy problems occur on the individual level, the impact of those actions is measured at the organizational level.[275] The NIST explains this contradiction away based on the argument that it is the organization that must account for the breadth of impact to many individuals rather than focusing only on each individual impact.[276] Costs to the organization are identified nonexclusively as those that are related to direct, noncompliance, reputational, and internal culture damages.[277] Using the PRM, an organization will identify its data actions, the potential harms to individuals, and possible negative outcomes to the organizations. Those outcomes are then ranked and priorities for remediation are set.[278]

C. PRM and Privacy Resilience

PRM is arguably an example of engineering resilience. First, it is system based; if resilience is defined as "the capacity of a system to

[270] *Id.* at 20–21.

[271] *Id.* at 22.

[272] *Id.*

[273] *Id.* at 54 app.E.

[274] *Id.* at 55 app.F.

[275] *Id.* at 23.

[276] *Id.*

[277] *Id.*

[278] *Id.* at 26 ("Thus, the PRAM provides a repeatable process that enables agencies to visualize where privacy risk may be occurring in their systems, communicate these risks at appropriate organizational levels, and make resource decisions with respect to addressing the risks.").

withstand internal and/or external change yet remain within the same regime"[279] then a system of privacy must first be conceived. By defining a common vocabulary and establishing engineering privacy objectives, the PRM facilitates communications between policy and technical fields and promotes privacy in cybersecurity systems. Thus, these definitions are an important foundation for privacy resilience. Feedback and updates are part of the privacy framework. The language and definitions will continue to be discussed, and the NIST plans to continue accepting comments and to hold future public workshops. In addition, the Framework will incorporate continual learning from the experiences of individual organizations. This adaptive capability is a hallmark of a resilient system.[280] Resilience planning decries a system that is a "cookie-cutter one-size-fits-all magic-bullet solution[]."[281] These factors contribute to privacy system adaptability, at least in part. In a smart city, the NIST Privacy Framework would be valuable because it does not depend entirely upon the FIPPs to define the system of privacy to be maintained. Broader concepts in the framework and in the definition of problematic data actions provide more flexibility for understanding and preserving what privacy means in the smart city.

The Privacy Risk Model places privacy conceptually within risk management and addresses it within the management of data systems, thereby operationalizing it within an organization.[282] In comparison, resilience planning also incorporates implementation protocols and internal controls based on evaluation of risk to a system.[283] However, the Privacy Risk Model does not explicitly incorporate privacy engineering objectives within the analysis, therefore significantly weakening its connection to privacy resilience. Furthermore, the Privacy Risk Model measures privacy impacts at the organizational rather than the individual level, balances factors in the model to favor organizational interests over individual interests in privacy, and does not require transparency. The lack of a transparency requirement is problematic, as it negatively affects the ability of society to discuss, address, and decide how privacy should be affected by information systems in a smart city. In that respect, the model fails to support privacy resilience because it prevents it from

[279] Ahjond S. Garmestani et al., *Can Law Foster Social-Ecological Resilience?* 18 Ecology & Soc'y 37, 37 (2013) (citing Holling, *supra* note 15).

[280] *See* Ruhl, *supra* note 229, at 1387–88.

[281] *See* Arnold, *supra* note 107, at 253.

[282] *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011) (discussing survey results concerning how companies are operationalizing privacy protecting policies to meet consumer expectations rather than placing an emphasis on strict rule compliance).

[283] *See* Andrea M. Matwyshyn, *Resilience: Building Better Users and Fair Trade Practices in Information*, 63 Fed. Comm. L.J. 391, 397 (2011) (discussing how individuals can become more resilient to cyber risk).

evolving within the social context in which it operates. Despite the feedback loops the framework incorporates, it cannot be viewed as a socio-ecological resilience approach for these reasons.

With regard to governance, the NIST Framework is voluntary and decentralized, and its evolution will include input from different sectors of society. The fundamental structure can be used across global legal boundaries and by different organizations. In this sense it meets the recommendation of some resilience scholars that suggest law should not be hierarchical and inflexible.[284]

The NIST Framework is not the only effort to take a privacy engineering approach. Nokia describes its proposed Privacy Engineering and Assurance program as part of an "engineering methodology to bridge the gap between laws and principles and technologies,"[285] and views it as an extension and implementation of Privacy by Design.[286] Nokia believes that a new professional discipline is necessary because of the digital environment, extensive data collection, and analytics that are "very powerful and enable unprecedented understanding of individual actions and behaviour."[287] Nokia includes Privacy by Design as one essential element for protecting privacy. Risk assessment and controls, management processes, and assurance activities for ensuring compliance are also required.[288] In sum, privacy engineering processes are intended to move Privacy by Design from the theoretical to practical implementation.[289]

The Centre for Information and Policy Leadership proposes a similar approach, emphasizing translational actions that would help implement privacy principles into actionable business realities.[290] Summarizing the need, the Centre states:

> As the pace of technological change outstrips the conventional thinking of lawmakers, regulators and businesses, it is suggested that a calibrated, risk-based approach may improve the ability of businesses to take a better-informed and better-structured approach to the handling of colossal volumes of personal information that they collect, receive, store, use and share on a daily basis.[291]

As an addition to laws and regulations, the Centre believes that a risk-based approach has "greater flexibility and more agility" to address fast moving technology and data collection.[292] Threat assessment, harm

[284] *See* Humby, *supra* note 202, at 97–98, 113.

[285] NOKIA, PRIVACY ENGINEERING & ASSURANCE: THE EMERGING ENGINEERING DISCIPLINE FOR IMPLEMENTING PRIVACY BY DESIGN 3 (2014).

[286] *See supra* Part II.D.

[287] *See* NOKIA, *supra* note 285, at 3.

[288] *Id.* at 5–6.

[289] *Id.* at 5 (providing that Nokia also proposes an entire discipline of certified professionals).

[290] *See* CTR. FOR INFO. POLICY LEADERSHIP, A RISK-BASED APPROACH TO PRIVACY: IMPROVING EFFECTIVENESS IN PRACTICE 2–3 (2014).

[291] *Id.* at 2.

[292] *Id.* at 4.

identification to both individuals and to society, and a matrix that maps threats to harms are all parts of the envisioned risk management system. The Centre report notes the decreasing effectiveness of regulators who have fewer resources for enforcement. Therefore, the privacy risk matrix could feed back into regulatory enforcement decisions in order to allocate these limited resources.[293] This proposal, with its emphasis on risk, a feedback loop, and the capacity for the system to learn, contains many aspects of engineering resilience and is similar to the NIST Framework.

D. Beyond Engineering Resilience

The NIST engineering privacy framework and similar frameworks could, and may, be used to build privacy survivability in a smart city, but they apply a narrower engineering resilience, or in some ways an ecological resilience approach that does not incorporate societal debate, and which generally elevates organizational and system efficiency over individual privacy. Although the NIST approach promotes privacy resilience by defining more broad based values that allow for flexibility and adaptability beyond inflexible FIPPs, by failing to incorporate individual privacy dialogues amongst citizens and their government, it fails to address how technology is changing society and how expectations of privacy could be affecting uses of technology. In a smart city, this inquiry is necessary in order to understand when circumstances push privacy beyond a threshold, incapable of maintaining its core identity.

Privacy in a smart city would be better addressed by applying a socio-ecological approach to resilience. This approach would seek to recognize the different states of privacy that may evolve from the pressures of today's data-driven world, and, in the same way that law is described as "a set of landscapes over which we find engineering and ecological resilience strategies mixing in different blends to form topographies of various contours depending on where in the system [one] look[s],"[294] privacy regulations, laws, principles, and norms may be applied in different contexts and to different threats. Conceiving privacy within the socio-ecological context of resilience would lend a methodology to the examination of a system of privacy, a framework for envisioning a complex system with not only one, but multiple thresholds. In applying a resilience framework to the city, there will be several thresholds of privacy: from emergency disaster access to health information to daily management of city waste. The effectiveness of bouncing back and the scope of adaptability will differ. Anticipating risks and planning for the

[293] *Id.* at 8–11.

[294] Ruhl, *supra* note 229, at 1383. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 479–81 (2006) (stating that "[p]rivacy seems to be about everything, and therefore it appears to be nothing[,]" and therefore proposing a more useful framework).

unpredictable, monitoring effects, and incorporating feedback opportunities that allow privacy thresholds to adjust are important.

Conclusion

In a future where a large portion of the population lives in cities, climate change, unpredictable disastrous events, and social instability make building a smart city an important goal for survival. Toward this goal, surveilling the environment, allocating resources based on data collection for personal use, and predicting future challenges all require the collection of massive amounts of data for analysis. This collection of massive amounts of data from personal and public spaces, and the use of that data for both population and individual planning, raises the question of whether privacy can exist within the smart city or whether it is too brittle and will break, ceasing to exist, because of the stresses imposed upon it. It remains to be determined whether privacy can survive and be resilient in the face of ubiquitous data collection and sensors in the smart city. As some scholars have noted, "[w]hile privacy is important, it is too narrow a concept to adequately address the risks of what big data projects can do."[295]

Methods to preserve privacy in the smart city deserve further study, and the resilience literature provides a robust approach to frame that study. This Article proposes, however, that privacy resilience should not only be considered from the engineering resilience viewpoint, which is the approach taken by FIPPs and in part by the NIST Privacy Framework, but rather, it must incorporate the complex relationships among privacy, social systems, and individual rights. When a privacy threshold is defined too narrowly, then entrenched expectations imagine only one vision of privacy. Rather, multiple thresholds should be envisioned as privacy adapts to changing conditions. In the smart city, FIPPs have little traction, are too simplistic, and are generally unrealistic. While selective laws banning sensitive data collection or use can meet expectations of privacy in the smart city for unique privacy thresholds, laws that globally ban the use of swaths of smart city technology or completely prohibit the identification of individuals are doomed to fail, thus setting up conditions for privacy to fail. Yet privacy in the smart city can be resilient if it is conceptualized as an adaptive system, capable of differing states that can evolve under different circumstances. The socio-ecological approach is the more relevant framework to apply to the study of whether privacy can be resilient in the smart city. Future work should analyze how society has engaged, or should engage, in discussions

[295] Crawford et al., *supra* note 171, at 4.

surrounding the multiple meanings of privacy,[296] design frameworks or systems that engage legal, ethical, and self-regulatory mechanisms based on these constructions, and integrate continual feedback loops so that principles of privacy can survive and develop along with the evolving nature of smart cities.

[296] Current studies from both academia and practice describe how consumers will share information and how they perceive privacy. *See* Ericsson, *Sharing Information: The Rise of Consumer Influence*, Consumer Insight Summary Rep. (Ericcson ConsumerLab), Sept. 2015 (discussing a study of smartphone users around the world and ways that they agree to share information); Mary Madden & Lee Rainie, Americans' Attitudes About Privacy, Security and Surveillance (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ ("The majority of Americans believe it is important—often 'very important'—that they be able to maintain privacy and confidentiality in commonplace activities of their lives."). For a summary and links to studies over time, see *Public Opinion on Privacy*, Electronic Privacy Info. Ctr., http://epic.org/privacy/survey/ (last visited Jan. 16, 2017).

***