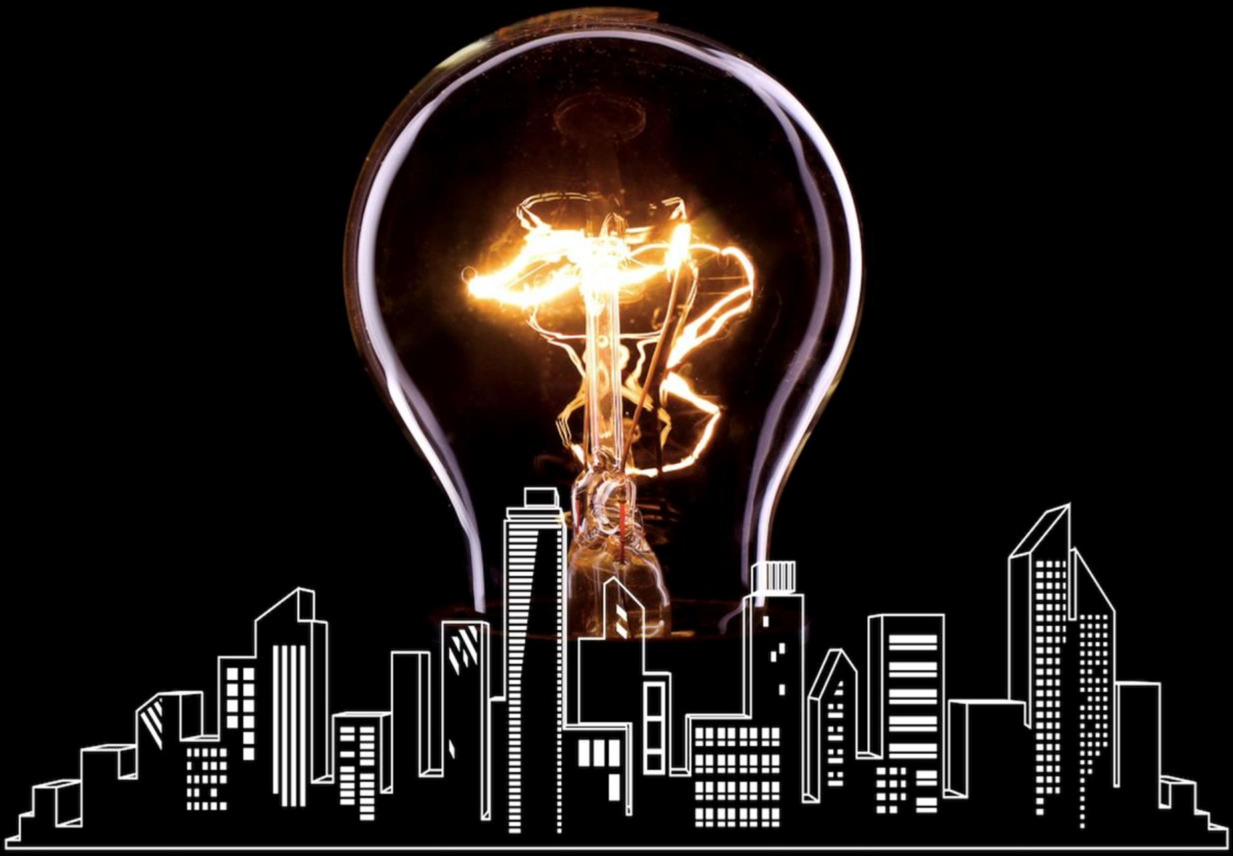
Race to the Future of American Cities

The Status of & Demand for Federal Smart City Legislation



"We will neglect our cities to our peril, for in neglecting them we neglect the nation."
– President John F. Kennedy

URBAN TECHNOLOGY SERIES:
An Independent Policy Series Presented by the
Chaddick Institute for Metropolitan Development
at DePaul University

AUTHORS:
Kirstin Anderson-Hall
Brandon Bordenkircher, MPA
Alexander Hall
Brady Penn

EXECUTIVE SUMMARY

Smart cities and the Internet of Things (IoT) are quietly becoming the most influential tech trends in the United States and has already revolutionized the way we live our lives. Some of the biggest potential consumers for this technology are cities and governments seeking to solve long standing problems in creative ways. These burgeoning smart cities face mounting pressure from their constituents and relatively little direction from state and federal authorities.

The purpose of this paper is to address the implications of the lack of federal action on issues pertaining to the Internet of Things (IoT) and smart cities and to educate audiences such as elected officials, tech industry professionals, and the general public on the potential benefits of these innovations.

INTRODUCTION

According to a recent United Nations report, 55% of the world's population currently lives in urban areas. By 2050, that percentage is forecasted to increase to 68%. This large influx of people moving into urban areas will create many challenges for elected officials (e.g. unemployment, crime, pollution), and it will likely increase strain on infrastructure and public services (e.g. public transit, energy grids). In short, public authorities will need to do *more* with *less*. The solution? Smart cities.

Anthony Townsend wrote an apt explanation of smart cities in his book "Smart Cities" [2013] writing that "smart cities are places where information technology is wielded to address problems old and new." Cities use this information technology to adapt in real-time, pulling data from sensors, sending that data to software that then gives us insight into how to fix a particular issue.

Smart cities may sound like an esoteric and futuristic idea, but a new wave of policies leveraging available technology are already being implemented and utilized in cities around the globe. Barcelona, Spain is using data to dramatically reduce traffic jams, pollution, and energy usage, while Las Vegas, Nevada is doing so to improve traffic flow. Birmingham, Alabama is working to reduce gun violence by using a high tech network to detect gunshots, and London, England is collecting data to solve pollution issues that cause 9,000 deaths annually. Further afield, Singapore is gathering data to aid the impending labor gap due to its aging population, and India is hoping to offer intelligent public services and connect billions of citizens to government services via information and communication technologies.

As the examples above demonstrate, smart cities have the potential to improve the quality of life for citizens. However, there are concerns about the implementation of smart city technology, particularly centering around privacy and security matters. As a result of these complexities, the U.S. Congress has introduced several bills in recent months that will help give companies and cities the freedom and support to innovate (via funding and coordination), while still laying down guardrails to mitigate potential negative externalities.

Those bills include:

- *The Smart Cities and Communities Act of 2019 (S.1398, H.R.2636)*
- *The Internet of Things Cybersecurity Improvement Act 2019 (S.734, H.R.1668)*
- *The DIGIT Act of 2019 (S.1611)*
- *The IoT Readiness Act of 2019 (H.R.3789)*
- *The IoT Standards Leadership Act 2019 (H.R.3811)*
- *The DASHBOARD Act of 2019 (S.1951)*

The purpose of this white paper is to inform smart city leaders, technology sector workers, elected officials, and the average citizen on the importance of this maturing technological space and the key aspects of the bills listed above and what they are designed to do. Before delving further into the bills, however, we first provide some additional background information about the promise and potential perils of smart cities.

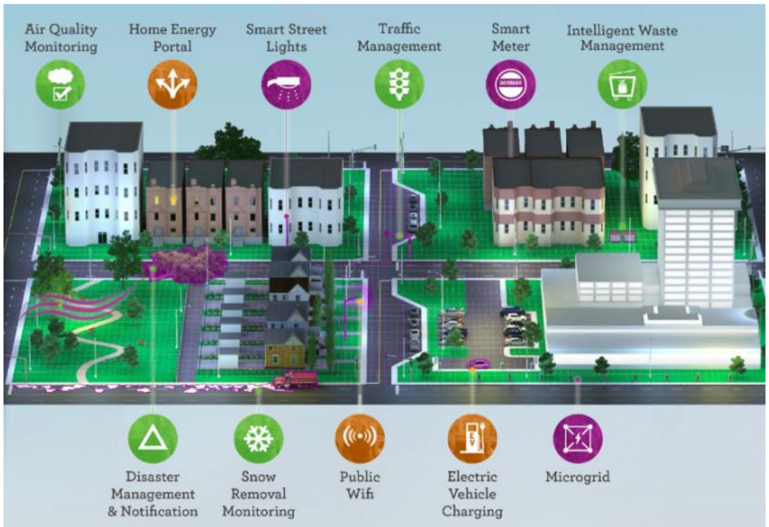
SMART CITY DEFINITION, BENEFITS & CONSIDERATIONS

It's hard to define exactly what a "smart city" is. Every city leader has a different understanding of what it means. Some leaders prefer to say, "connected communities," while other leaders don't think tech needs to be included in the definition at all, as many smart city efforts (involving affordable housing, improved infrastructure, increased bikeshare, etc.) don't necessarily rely on internet of things tech. It is likely that the definition will continue to evolve as a background paper from the UK Department for Business, Innovation and Skills stated in 2013: "The concept is not static, there is no absolute definition of a Smart city, no end point, but rather a process, or series of steps, by which cities become more 'liveable' and resilient and, hence, able to respond more quickly to new challenges." Another description put forward by consulting firm Frost and Sullivan listed eight key factors necessary for a city to be considered "smart"; they included smart governance, smart energy, smart building, smart mobility, smart infrastructure, smart technology, smart healthcare and smart citizen. The illustration from Bronzeville Community of the Future [Figure 1] lists smart city components as air quality monitoring, home energy portals, smart street lights, traffic management, smart meters, intelligent waste management, disaster management and notification, snow removal monitoring, public wifi, electric vehicle charging, and microgrids.

> *The purpose of this white paper is to educate smart city leaders, technology sector workers, elected officials, and the average citizen on why this maturing technology is important and why these bills are necessary to the future of our country.*

For the purposes of this paper, we define smart cities as localities that utilize information technology by gathering data from the physical world via the Internet of Things (i.e. any device that connects to the internet; which consists of sensors, beacons, cameras, applications, and smartphones). The data collected by these devices would traditionally be stored and utilized within industry value chains (i.e. Product Systems). For example, an air-condition is equipped with sensors to let the manufacturer and user know when the product is in need of repair.

FIGURE 1: Bronzeville Community of the Future Illustration



Source: Commonwealth Edison Company, 2017. All Rights Reserved. Reproduced with permission.

With advances in storage, computation, and artificial intelligence, the data from the air-conditioned will now have the ability to be shared *outside* of its traditional value chain by sending and receiving information to balance the flow of electricity based on electric grid use. The smart electric grid would then send information to the air-condition by turning it down or off to avoid a citywide blackout due to equipment overload.

Utilizing this information outside of its industry value chain creates new opportunities by forming a customer focused ecosystem called a Human-Centric System of Systems. The data is shared (via cloud infrastructure) and analyzed (via machine learning) to create value by looking beyond existing product-based business models in order to solve problems, create new products, and generate best practices that result in more efficient government services and a better quality of life for all citizens.

Data has become the ultimate control point to help organizations (i.e. cities and companies) leverage their resources in the most effective way. With all this data in motion, there are several important areas of consideration for policymakers: namely, how to best legislate cyber-physical security, IoT industry standards (both in the U.S. and internationally), privacy issues and data rights.

Cities, states, and the federal government have different views on how to regulate these issues and this has often caused a push and pull between their differing interests. Cities have traditionally been the arbiters of urban design and improvement while federal and state dollars have served to encourage certain initiatives or allow for more equitable development between different sized communities. While cities often solve these problems in a piecemeal fashion, federal attention can lead to massive increases in the speed of change. Similarly, smart city strategies and policies look likely to be decided primarily at the local level. In fact, several cities have already launched their own smart city initiatives, despite the fact that the federal government has yet to take substantial action and pass any IoT bills.

In fact, several cities have already launched their own smart city initiatives, despite the fact that the federal government has yet to take substantial action and pass any IoT bills.

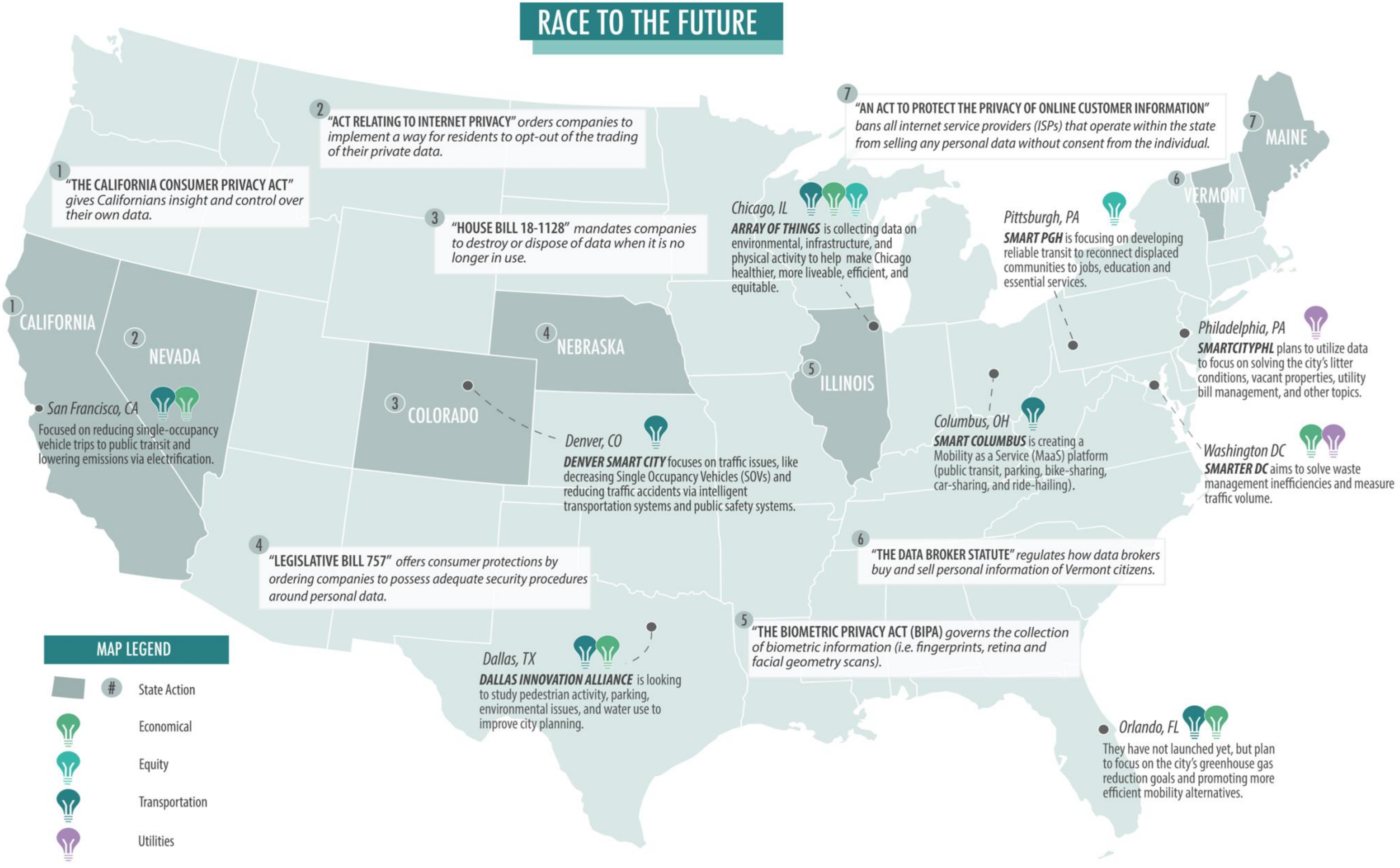
EXAMPLES OF SMART CITIES IN THE U.S.

The number of IoT-connected devices is expected to grow from 6.6 million in 2016 to 22.5 billion by 2021 as the prices for IoT devices, storage, and computing continues to fall. This growing accessibility of IoT-devices means the number of smart city initiatives and the amount of cyber-physical data will increase. According to the Smart America Challenge, city governments are projected to spend upwards of $41 trillion over the next 20 years on smart technology to upgrade their infrastructure. Already, many U.S. cities are utilizing various smart city solutions and optimizing data from the cyber-physical world in order to fix a wide variety of problems and ultimately make their cities more efficient and livable. Please refer to the map [Figure 2] on page 4.

Chicago, IL

Chicago's Array of Things (AoT) is an IoT project featuring 200 nodes (i.e. sensors and cameras) that collect real-time data on environmental, infrastructure, and physical activity in order to measure livability factors in Chicago (e.g. climate, air quality and noise). This information is published as open data for public use and research purposes with the ultimate goal of helping engineers, scientists, policymakers and residents make decisions

FIGURE 2: Examples of U.S. Smart Cities and State Privacy Legislation



1 **"THE CALIFORNIA CONSUMER PRIVACY ACT"** *gives Californians insight and control over their own data.*

2 **"ACT RELATING TO INTERNET PRIVACY"** *orders companies to implement a way for residents to opt-out of the trading of their private data.*

3 **"HOUSE BILL 18-1128"** *mandates companies to destroy or dispose of data when it is no longer in use.*

4 **"LEGISLATIVE BILL 757"** *offers consumer protections by ordering companies to possess adequate security procedures around personal data.*

5 **"THE BIOMETRIC PRIVACY ACT (BIPA)** *governs the collection of biometric information (i.e. fingerprints, retina and facial geometry scans).*

6 **"THE DATA BROKER STATUTE"** *regulates how data brokers buy and sell personal information of Vermont citizens.*

7 **"AN ACT TO PROTECT THE PRIVACY OF ONLINE CUSTOMER INFORMATION"** *bans all internet service providers (ISPs) that operate within the state from selling any personal data without consent from the individual.*

San Francisco, CA
Focused on reducing single-occupancy vehicle trips to public transit and lowering emissions via electrification.

Denver, CO
DENVER SMART CITY focuses on traffic issues, like decreasing Single Occupancy Vehicles (SOVs) and reducing traffic accidents via intelligent transportation systems and public safety systems.

Dallas, TX
DALLAS INNOVATION ALLIANCE is looking to study pedestrian activity, parking, environmental issues, and water use to improve city planning.

Chicago, IL
ARRAY OF THINGS is collecting data on environmental, infrastructure, and physical activity to help make Chicago healthier, more liveable, efficient, and equitable.

Columbus, OH
SMART COLUMBUS is creating a Mobility as a Service (MaaS) platform (public transit, parking, bike-sharing, car-sharing, and ride-hailing).

Pittsburgh, PA
SMART PGH is focusing on developing reliable transit to reconnect displaced communities to jobs, education and essential services.

Philadelphia, PA
SMARTCITYPHL plans to utilize data to focus on solving the city's litter conditions, vacant properties, utility bill management, and other topics.

Washington DC
SMARTER DC aims to solve waste management inefficiencies and measure traffic volume.

Orlando, FL
They have not launched yet, but plan to focus on the city's greenhouse gas reduction goals and promoting more efficient mobility alternatives.

that help Chicago become healthier, more livable, efficient, and equitable.

Columbus, OH

The City of Columbus' Smart Columbus initiative is funding nine projects funded by a $40 million grant from the U.S. DOT and $10 million from Vulcan Inc. The initiative seeks to create a Mobility as a Service (MaaS) platform that allows residents to pay for all modes of transportation (public transit, parking, bike-sharing, car-sharing, and ride-hailing) through one app to improve mobility. A second project looks to allow semi-autonomous freight trucks to communicate in real time so they can closely follow one another, resulting in saved fuel, increased vehicle safety, and improved traffic flow.

Dallas, TX

The City of Dallas has launched the Dallas Innovation Alliance, a 501c(3) public-private partnership powered by AT&T. The project consists of a downtown four-block corridor featuring nine integrated smart city projects and is hailed as the fastest-to-market smart cities initiative in the country. The project utilizes digital infrastructure nodes, pedestrian sensors, public wifi, smart parking, environmental sensors, smart water metering, and interactive digital kiosks to improve the use of data in city planning. The following are examples of U.S. smart cities and not a definitive list.

Denver, CO

The City of Denver has formed a public-private partnership with Panasonic to use data and modeling alongside identified residents pain points. The partnership focuses on traffic issues like decreasing Single Occupancy Vehicles (SOVs) and reducing traffic accidents (Vision Zero Initiative) by integrating intelligent transportation systems and public safety systems.

Orlando, FL

Orlando announced that it is seeking a consultant to create a comprehensive smart city strategy to coordinate efforts and shape a single vision. This move hopes to help the city evaluate technology options and find cost-effective tools. There will be a large focus on the city's greenhouse gas reduction goals and promoting more efficient mobility alternatives.

Philadelphia, PA

Philadelphia entered into the smart cities space in 2017 with their SmartCityPHL program. The city developed a smart city advisory committee prior to leaping into larger projects, but instead of investing in typical "smart" technologies, the city hosted community workshops to brainstorm ideas to help form their roadmap. Data will play a large role in overall strategy, and will focus on the city's litter conditions, vacant properties, utility bill management, and other topics.

Pittsburgh, PA

The City of Pittsburgh has launched Smart PGH which seeks to use technology to develop safe, reliable transit to reconnect displaced communities to jobs, education and essential services. Areas of focus include: mobility optimization to reduce emissions, smart street lights (equipped with sensors), autonomous shuttles, and data collection/platforms/process framework.

San Francisco, CA

San Francisco is focused on a mode shift from single-occupancy vehicle (SOV) trips to public transit; lowering emissions via electrification and demand management; and solving transportation equity. The city is looking to accomplish these goals by implementing shared, autonomous, connected, electric, transportation to streamline and synchronize traffic and eliminate parking to create room for green spaces and affordable housing.

Washington, D.C.

The Smarter DC initiative aims to help define smart city governance frameworks, interoperability standards, and models for replication, scalability, and sustainability. Problems it seeks to solve include Smart

Waste Management by adding sensor technology to waste cans to provide data on fill levels allowing the DPW to identify waste collection inefficiencies, and movement analytics using video sensors to classify and count city movement (people, bikes, cars, etc.) to measure traffic volume and flows in key economic development corridors.

SMART CITY & IoT RELATED BILLS IN CONGRESS

While countries like India and Singapore invest $7.4 billion and $7.5 billion, respectively, into their smart city initiatives, the U.S. federal government lags behind with a total of $240 million invested for two smart city initiatives back in 2016. In addition, the Congressional Caucus on the Internet of Things, and the House-based Smart City Caucus, were created in 2017 to educate members of Congress on smart city issues, IoT use cases, potential issues with the growing number of IoT devices and systems, and the policy issues surrounding the collection of consumer data by IoT devices. These are great first steps; however, as more cities start to implement their own smart city initiatives, it's important that IoT technology be funded and implemented properly as well as regulated in a thoughtful and coordinated manner.

Several of these bills are most likely to be passed piecemeal as additions to a larger infrastructure bill that may be the best chance at bipartisan policy making in the near future. The bills discussed in this paper include: *The Smart Cities and Communities Act of 2019; the Internet of Things Cybersecurity Improvement Act 2019; the DIGIT Act of 2019; the IoT Readiness Act of 2019; the IoT Standards Leadership Act 2019; and the DASHBOARD Act of 2019.*

Federal Coordination, Investment & Innovation: "The Smart Cities and Communities Act"

Introduced initially by Senator Maria Cantwell [D-WA], the Smart Cities and Communities Act of 2019 seeks to promote the use of smart technologies and systems via federal support for local technology initiatives. Ensuring smart city technology is understood and accessible to governments of all sizes will help policy makers create well informed and effective investments which will draw new businesses, create jobs, and enhance critical infrastructure.

The Smart Cities and Communities Act of 2019 would authorize $220 million for smart city investments each year for the next five years. It would focus on improving coordination of smart city programs and expanding their benefits to smaller under resourced communities. Among its many impacts the bill would foster a structure of reporting; help develop IoT sector jobs in cities big and small; improve smart city technology's quality, performance and safety; and foster international collaboration and trade of smart city technologies.

The bill also seeks to increase cross-city coordination around the U.S., create unified oversight, and consolidate the individual smart city elements the federal government is already working on (i.e. electric vehicles, autonomous vehicles, artificial intelligence, internet of things (IoT) devices, broadband access, smart grids, and data privacy).

The oversight and interagency collaboration required within the bill is substantial. Among other things, the proposal would require reports on the bill's implementation to the Committees on Commerce, Science, and Transportation and Energy, and Natural Resources in the Senate. It would also require reports to the Committees on Energy and Commerce, Transportation, and Infrastructure in the House. These measures are unlikely to be implemented anytime soon as political differences have caused a massive slowdown in comprehensive lawmaking. The funds for the proposal have also led it to flounder with Democrats and Republicans disagreeing on where funds would be drawn from according to those close to the issue. In spite of the Bill's long shot at passing, smart city funding is already flowing from agencies at every level of government.

Some of the most vehement supporters of smart cities foresee a future federal government agency which would focus solely on IoT and smart city management. Until this type of policy is consolidated and streamlined in such a way, however, we are likely to see funds coming from a plethora of government agencies.

Some of the programs already under development and application through various federal organizations include BroadbandUSA, Boulder Wireless Testbed, Big Data Regional Innovation Hubs, All of Us Research Program, Advanced Grid Modeling, Array of Things, Advanced Distribution Management Systems and Accelerate R2 Network Challenge. The sheer number of initiatives and programs illustrates the impact that a federal bill may have in encouraging information sharing and collaboration.

The Smart Cities and Communities Act was developed in collaboration with cities across the country, as well as telecommunications and information technology companies. In fact, many cities around the country have extensive smart city initiatives underway (per earlier examples).
Businesses and organizations, like the BSA - The Software Alliance, have shown support for this bill as they are eager to get a piece of this fast growing field. A recent survey by TechRepublic found that over 90% of businesses favor federal legislation including 62% of public safety technology firms and 50% of communication firms. Among these firms, Qualcomm has put federal efforts into creating the Smart Cities Caucus and pushing for legislation such as the Smart Cities and Communities Act. Among the numerous businesses interested in this field, Reinvently, Vates, Fusion Informatics and others represent the startups banking on the massive upside potential of IoT and smart cities.

The Senate bill (S.1398) was referred to the Committee on Commerce, Science, and Transportation in on 5/9/2019 and appears likely to die there. As of now, the chair of this committee refuses to bring it to a vote. On 5/9/2019 the House bill (H.R.2636) was referred to: the Energy and Commerce; Science, Space, and Technology; Education and Labor; Foreign Affairs. In order to move on, the bill will need to be referred out by the Speaker.

Security Requirements: "The Internet of Things Cybersecurity Improvement Act"

In 2016, the Mirai botnet attack took down several popular websites by scanning the Internet for IoT devices, logging into those devices where the default username-and-password combo were not changed, and infecting them. The Mirai botnet attack involved a hundred thousand hijacked IoT devices to bring down Dyn (an internet performance management and web application security company).

Since this attack, Congress has made attempts to pass legislation around IoT security, including a failed attempt in 2017 that looked to prevent the government from buying connected devices that had blatant security weaknesses. The Internet of Things Cybersecurity Improvement Act of 2019, introduced by Sen. Mark R. Warner [D-VA] in the Senate and Rep. Robin Kelly [D-IL] in the House, aims to build a framework to institute a list of requirements for secure connected devices, federal agencies, contractors, and vendors.

The bill designates the responsibility of setting the requirements for secure development, identity management, patching, and configuration management for IoT devices to the National Institute of Standards and Technology (NIST). From there it will be the responsibility of Office of Management and Budget (OMB) to issue guidelines for each federal agency that are consistent with the NIST requirements and require OMB to review those policies every five years (at a minimum). It will also require any IoT device purchased by the federal government to comply with the NIST requirements.

NIST will also be required to cooperate with Department of Homeland Security (DHS), cybersecurity researchers, and industry experts to write reports advising on IoT device weaknesses to guarantee any vulnerabilities are rectified. It will also demand U.S. government information systems vendors sign disclosure policies, so if a weakness in an IoT device or information system is uncovered, it can be fixed.

It is a serious issue when a single person's bank account is hacked; IoT technology opens up society to the even greater threat of an entire cyber-physical infrastructure being hacked (i.e. the energy grid of an entire region of a country). The implications of the latter could cause cacophony and potentially result in deaths. These implications make an IoT cybersecurity bill *crucial* to our nation's safety.

The Congressional Budget Office (CBO) estimates the bill would cost $35 million over the 2019-2024 period, assuming appropriation of the necessary amounts. Senate bill S.734 and House bill H.R.1668 are currently in conference, awaiting a compromise. The language causing the holdup: the House bill defines what an IoT device is, while the Senate removed the definition of what an IoT device is. One other difference between the bills: the Senate bill covers coordinated security disclosures for *all* types of technology, while the House bill just covers disclosures for IoT devices.

Regulation & Cross-Sector Collaboration: "The Digit Act"

On 5/22/2019, Sen. Deb Fischer [R-NE] reintroduced a stalled 2017 bill that would promote the Internet of Things industry in the U.S. which includes several provisions that encourage lawmakers to nurture connected technology instead of stifling its development. The DIGIT Act (Developing Innovation and Growing the Internet of Things Act) would create a working group, including federal and private-sector individuals, that will work to identify policies in relation to the IoT, such as spectrum needs, consumer protection, privacy and security, and regulatory environment.

Moreover, The DIGIT Act would help ensure the nation's preparedness for communication technologies of the future as Congress estimates that 125 trillion devices will be connected to the internet by 2030, with IoT having the potential to generate trillions in new economic activity worldwide. The working group would also identify policies that would improve coordination among federal agencies with jurisdiction over the IoT. If passed, oversight of the IoT would fall under many regulatory bodies; for example, the Food and Drug Administration would regulate medical wearables, while the National Highway Traffic Security Administration's jurisdiction would manage connected cars.

The Department of Commerce, in particular, would have its own steering committee to advise the working group (along with its subset of agencies). The committee's recommendations would be under the purview of identifying federal regulations and statutes, grant practices, programs, and budgetary and jurisdictional practices and to identify situations in which the use of IoT could deliver stable economic and societal benefits to the United States in the form of smart transit and transit technologies, augmented logistics and supply chains, healthcare and public safety to name a few. Furthermore, the DIGIT Act would require the Federal Communications Commission (FCC) to complete a report that assesses the spectrum needs required to support the IoT.

According to the CBO, it will cost an estimated $3 million to fund the necessary working groups proposed by the DIGIT Act. Costs would be distributed among the respective participating agencies and would be subject to the availability of appropriated funds. Supporters of the DIGIT Act include: The App Association, the U.S. Chamber of Commerce, CTIA, the Competitive Carriers Association, the Computing Research Association, the Consumer Technology Association, the Information Technology Industry Council, the Information Technology and Innovation Foundation, the Semiconductor Industry Association, the Telecommunications Industry Association and VMware. The bill (S.1611) is currently in the Committee on Commerce, Science, and Transportation awaiting amendments.

Wireless Infrastructure: "The IoT Readiness Act"

The United States needs to ensure our country's wireless infrastructure is ready for the surge of IoT devices. The IoT Readiness Act of 2019 is a House bill that mandates that the Federal Communications Commission (FCC) create a biennial report for Congress on the growing use of the IoT devices and gadgets that utilize 5G mobile networks.

Wireless signals (i.e. TV broadcast, radio stations, GPS devices, and cell phone service) travel over airwaves via a finite radio frequency called spectrum. No two devices can transmit over the same spectrum/frequency at the same time in the same area – if they did, they would cause interference. If the available spectrum cannot sustain the number of devices, the signals will inevitably interfere with each other and fail, making the entire idea of smart cities moot.

In countries like China and South Korea, 5G networks and IoT devices are being deployed at a breakneck speed due to a lack of restraint and concern for privacy/use cases (i.e. surveillance). Meanwhile, citizens in the U.S. have been bombarded with a Russian disinformation campaign, care of RT (a television network funded by the Russian government), claiming 5G causes "brain cancer, infertility, autism, heart tumors and Alzheimer's disease." These unsubstantiated concerns have already attempted to stunt the rollout of 5G across the U.S. with a coalition of 52 grassroots organizations calling on the Federal Communications Commission (FCC) to delay deployment of 5G infrastructure citing health claims that lack scientific support.

China's current IoT policy could potentially add $196 billion US dollars to its cumulative GDP in manufacturing industries over the next 15 years. Considering IoT's far-reaching impact on the future of the U.S. economy, it is crucial that our country build out its own 5G infrastructure to support the growing spectrum demand for IoT devices. The IoT Readiness Act (H.R.3789) was referred to the House Committee on Energy and Commerce on 7/17/2019.

Setting International IoT Standards: "IoT Standards Leadership Act"

The IoT Standards Leadership Act was introduced by Rep. Doris Matsui [D-CA] & Mike McCaul [R-TX] in 2019 with a focus on fostering U.S. leadership and participation for setting international IoT standards. The bill would require the U.S. Department of Commerce to study the U.S. involvement in the international IoT standards-setting processes and foreign countries' IoT standards, with a focus on cybersecurity and risk management.

Being leaders in setting IoT standards not only affects U.S. manufacturers – it will also shape global competitors who want access to the U.S. market. According to Abraham Newman & Daniel Nexon, "to really affect the global economy through such standard-setting, a government requires the necessary regulatory expertise to identify and enforce market rules." The U.S. is a true "market great power" not only due to our extensive regulatory experience, but also because we are one of the largest markets in the world. However, the U.S. isn't the only leader in international standard-setting. U.S. companies have to abide by an array of laws in the European Union when it comes to trust-busting, environmental protections, and digital privacy. These regulations affect the practices of U.S. companies looking to operate in the EU and beyond which leads to global standardization of their operations.

The harmonizing of regulatory standards of the U.S. and EU would put immense pressure on other markets and will help prevent country-specific standards from hindering the progress of American innovation. H.R.3811 was referred to the House Committee on Foreign Affairs on 07/17/2019.

Data Value, Transparency & Privacy: "The Dashboard Act"

Smart cities, by function, deal with a deluge of data, which means there is greater potential for data privacy issues. Many tech companies including Facebook, Google and Twitter have built lucrative businesses off their users' personal information by offering a "free" product by allowing advertisers to target ads based on user habits. Several CEO's, including Facebook CEO Mark Zuckerberg, have been called to Capitol Hill and criticized for their companies' data practices; in fact, Facebook was forced to pay a $5 billion fine as a result of a settlement with the Federal Trade Commission (FTC). However, Congress has not yet been able to turn these criticisms into a bill.

Both Congress and President Trump have shown interest in a national consumer data privacy law to protect people's online privacy, but lawmakers continue to disagree on various components of the bill (i.e. enforcement, giving consumers the ability to sue companies that violate the federal law, allowing the FTC more authority to create rules on privacy, and whether or not the federal law will preempt the state laws).

However these concerns did not stop Senators Mark Warner [D-VA] and Josh Hawley [R-MO] from introducing the DASHBOARD Act (Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data) (S.1951) in the Senate in June 2019. This bill would require tech companies to determine the value of the data they collect and provide easy options for users to opt out of companies sharing and/or selling their personal data. The bill would require social media platforms with over 100 million monthly active users to send their users reports laying out the economic value of their data, the types of data points collected, supply a list of the third parties utilizing the data, and compile an annual report on the aggregate value of user data.

It would also authorize the Securities and Exchange Commission (SEC) to create a methodology for calculating a value for user data. In addition, it gives users the ability to delete any of their data, either completely or via specific type. This increase in transparency and disclosure has the potential to provide antitrust regulators additional insight into potentially anti-competitive practices.

Several leaders in the tech space have said this bill is inherently flawed due to the potential burden it places on social media companies, the fact that most users forgo monetary rewards to avoid even *thinking* about privacy, and that our data might not be worth very much when it stands alone.

States Passing Their Own Privacy Laws

As we wait for a federal data privacy law, a few states (see below) have decided to take up the mantle themselves. Although these state laws are a step in the right direction, industry groups, like the Internet Association (whose members include Google, Facebook and Amazon), have launched an ad campaign warning about 50 individual state privacy laws, and flooded D.C. to pressure Congress to pass a national privacy law (which would include a provision to supersede all state privacy legislation). In addition to the Internet Association, the chairman of the FTC, the top privacy regulator in the country, has also urged Congress to pass a national law. Please refer to the map [Figure 2] on page 4.

California

"*The California Consumer Privacy Act*" (CCPA) will give consumers the ability to know what personal information of theirs has been collected by for-profit companies, how their data is used, and know to whom it has been sold or disclosed. It also gives consumers the ability to access and control their own information and to whom the data is sold.

Colorado

House bill 18-1128 mandates that companies who manage user data destroy or dispose of data when it is no longer in use. It also requires data breaches to be reported within 30 days. Additionally, if said breach impacts more than 500 Colorado residents, the Attorney General of the state must be notified within that same time period.

Illinois

"*The Biometric Privacy Act (BIPA)*" governs the collection of biometric information (i.e. fingerprints, retina and facial geometry scans). The law allows individuals to file a lawsuit for damages if a violation transpires (i.e. not securely storing biometric data, not obtaining consent for data collection and not destroying biometric identifiers in a timely manner).

Maine

"*An Act to Protect the Privacy of Online Customer Information*" bans all internet service providers (ISPs) that operate within the state from selling any personal data without consent from the individual. This can include browsing history and application usage information.

Nebraska

Legislative bill 757 offers consumer protections to it the residents of the state by ordering companies to possess adequate security procedures around personal data and ensure that third parties who access the data also have security measures in place.

Nevada

Nevada's "*Act relating to Internet Privacy*" updates the existing internet privacy law to order companies to implement a way for residents to opt-out of the trading of their private data. Businesses must give either a way to opt-out online or a toll-free telephone number.

Vermont

"*The Data Broker Statute*" regulates how data brokers buy and sell personal information of Vermont citizens. Additionally, it requires all firms that sell or license data to register annually with the Vermont Attorney General, disclose operational information and report data breaches.

General Data Protection Regulation

As the United States defers on passing a comprehensive federal data privacy law, the European Union was able to successfully pass its own in 2016, which went into effect May 2018. Like the DASHBOARD Act, one of the core focuses of the *General Data Protection Regulation* (GDPR) is the strengthening of consent; however, GDPR offers greater protection by requiring that companies use simple language, that consent for data be applied individually, and that a protection for children be available (in the form of parents being able to opt in to data collection on their child's behalf). Companies are also required to notify the authorities and consumers of a data breach within 72 hours of becoming aware of it. GDPR offers citizens more control in accessing their personal data stored by companies, the ability to have their data erased and bar third parties from processing it, and the opportunity to take their data and transfer it to a different service provider.

This law not only affects organizations located within the EU, but it also applies to institutions outside of the region that offer goods or services, or that monitor the behavior of users.

Breaching GDPR carries a hefty fine equating to 4% of annual global turnover or €20 million euros (roughly $23 million). As big technology firms update their respective data standards to adhere to GDPR law, data privacy advocates in the EU continue to question whether these organizations are in full compliance. Earlier this year, Google was issued a fine of $50 million by the French based data protection organizations The National Commission of Informatics and Civil Liberties (CNIL), which claimed that Google had failed to comply with GDPR standards when new Android users set up their phones to follow onboarding processes. A handful of other large firms such as Amazon, Apple, and Netflix have been subject to complaints from data privacy organizations and activists based in the EU.

Creating a national data privacy law is necessary in order to maintain transparency, safety, and ownership of consumer data and privacy. Unlike the E.U.'s GDPR, the U.S.'s DASHBOARD Act which would act as a standard and foundation for national data management was referred to the Committee on Banking Housing and Urban Affairs on 10/24/2019 and has been read on the floor but is likely to die in committee.

MOVING FORWARD

This report serves as a reflection of our current predicament, as Congress considers smart city and IoT legislation and struggles to come to consensus. It is important that Congress continues to work closely with IoT device makers, cloud infrastructure companies, data rights groups, and local municipalities both big and small. Smart cities – and the IoT technology that drives them – have the potential to solve big problems and improve the quality of life for *all* citizens. It is imperative that the right legislation is enacted promptly, in an intentional manner, with the given flexibility to amend bills as technology advances.

> *Smart cities – and the IoT technology that drives them – have the potential to solve big problems and improve the quality of life for all citizens. It is imperative that the right legislation is enacted promptly, in an intentional manner, with the given flexibility to amend bills as technology advances.*

Anger at tech companies has only resulted in a single new law in recent years – a bill to prevent sex trafficking online. Although tech issues do not drive most voters to the polls, these innovations will have a *significant* impact on the U.S. economy, including jobs and economic growth, which is why there needs to be more IoT and smart city education for both elected officials and citizens. Cities are already using IoT technology to reduce traffic jams and energy usage; to help prevent gun violence; to reduce pollution; to solve the aging labor gap; and to connect billions of citizens to government services. Citizens need a basic understanding of why this technology is beneficial, this increased awareness could help ensure the continued funding and implementation of smart city solutions that will make our country and our world a better place.

In a 1962 speech, President John F. Kennedy asserted, "we will neglect our cities to our peril, for in neglecting them we neglect the nation." This quote is more relevant than ever at this point in our world history as populations continue to move to urban areas.

As the President and Congress weigh infrastructure spending, the neglect of IoT/smart city innovation and regulation puts our nation's security, economy, and future in peril. Other nations will be quick to take up the baton and cross the finish line if the American government remains sidelined. In order for us to lead this race, we need to make sure that we are participating. Studies, funding, and proactively setting thoughtful IoT standards, both in the U.S. and internationally, will help secure more efficient government services, cleaner cities, and a more equitable future for all U.S. citizens.

The starting gun has been fired. It is time for the U.S. to pick up the pace.

AUTHOR INFORMATION

Kirstin Anderson-Hall
Principal at 12 Tone Consulting
A Southern California native residing in Washington D.C. Her interests focus on utilizing social impact, civic engagement, and technology for the greater good. An American University masters graduate that has written several white papers spanning a wide range of tech policy issues.

Brandon Bordenkircher, MPA
CEO at 12 Tone Consulting
Chicago based tech policy leader with years of policy, government affairs, and research experience. His expertise focuses on local governments' response to disruptive technologies. He has worked for SHARE NOW (car2go), Airbnb, SmartStubs, and DePaul University's Chaddick Institute.

Alexander Hall
Independent Researcher
Alexander has a passion for studying the intersection between new technologies and communities. He has led local community engagement initiatives for billion-dollar tech companies as a Los Angeles resident.

Brady Penn
CEO at Telegraph Hill Solutions
A technology and public policy expert based in San Francisco. His work spans US and Australian politics and has included some of the biggest names in technology and government.

ACKNOWLEDGEMENTS

The writing of this report was a collaborative effort that was edited and formatted by **Mallory Livingston**, with additional research provided by **Ali Fendrick**, and title image created by **Kristiana Mitacek**. This paper was published by The Chaddick Institute on 1/31/2020.

The writers are especially grateful to the many congressional staffers that took the time to answer our questions. In addition, the following people were indispensable for providing their support and insights:

- Chelsea (McCullough) Collier: Founder at Digi.City
- Jessica Kupets: Program Manager at DePaul University's Chaddick Institute
- Jochen Renz: Advisor, New Mobility at Rocket Wagon Venture Studios
- Joe Schweiterman: Director at DePaul University's Chaddick Institute
- Julia Kanouse: CEO at Illinois Technology Association
- Ken Hejduk: COO at Sway Mobility
- Kristin Musulin: Senior Editor at Smart Cities Dive
- Olivia Pantoja: Consultant at the Concensus Group
- Paula Robinson: President at Bronzeville's Community Development Partnership
- Rajesh Sankaran: Research and Development Lead at the Array of Things
- Ron Rumack: Executive Director at Wisconsin IoT Council
- Sasha Bernhard: Senior Policy Advisor at Congresswoman Suzan K. DelBene
- Scott Smith: Assistant Director at DePaul University's Chaddick Institute
- Skip Newberry: President and CEO at Technology Association of Oregon