ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Balancing Privacy and Innovation in Smart Cities and Communities

ASHLEY JOHNSON I FEBRUARY 2023

Smart city technology could modernize local government services and improve residents' quality of life. To reap these benefits and maintain public trust, cities and communities need to balance the interests of innovation and privacy.

KEY TAKEAWAYS

- Data collection is what powers smart cities and communities, but it is also the source of privacy concerns—some legitimate and some based on unlikely worst-case scenarios.
- Many smart city technologies do not collect any data on residents' individual behavior or activities, instead collecting data on local infrastructure, the environment, or residents' collective behavior, which poses little to no privacy risk.
- Cities and communities need to balance concerns over cybersecurity risk, commercial use of data, and potential government surveillance against other concerns, including public safety, sustainability, beneficial uses of data, and cost.
- Congress should pass comprehensive federal data privacy legislation that would address many of the concerns arising from the commercial use of smart city data, and state lawmakers should regulate police use.
- Cities and communities should prioritize cybersecurity and take steps to protect residents' privacy, such as anonymizing personal data and setting rules for the companies they partner with on smart city projects.

CONTENTS

INTRODUCTION

Smart cities and communities can improve their residents' quality of life by using sensors, data, and analytics to optimize traffic and public transportation, better address crime, monitor sewers and waste, and manage the electric grid and other essential systems. Privacy advocates warn that smart cities and communities encroach on civil liberties. These fears are overblown, but balancing the interests of innovation and privacy will nonetheless be a key task for policymakers.

Most smart city applications are built around the Internet of Things (IoT): physical objects embedded with sensors or actuators and network connectivity to enable them to send, receive, and act on data. Other enabling smart city technologies include wired and wireless broadband networks, analytics tools to process data coming from sensor networks, and autonomous systems.

With these capabilities, smart cities and communities can collect and analyze vast quantities of data to automate processes, improve service quality, and make better decisions. In other words, this data collection is what makes cities and communities "smart." It can generate cost and time savings, increased productivity, and public health and safety, which would benefit governments, residents, and visitors alike to smart cities and communities. Smart city technologies can even help cities and communities address climate change by reducing their emissions.[1]

But smart cities' data collection is also the source of privacy concerns when the data collection involves personally identifiable information. Smart city technologies that collect data about residents, particularly sensitive data—such as personal information that could be used for identity theft—make attractive targets for cybercriminals. Moreover, every Internet-connected device involved in collecting, transmitting, or receiving smart city data is a potential security vulnerability, making cybersecurity integral in protecting residents' data privacy.

Additionally, privacy advocates have concerns over smart cities and communities that share the data they collect with private partners to defray the cost of deploying smart city technologies, or for other purposes. Some opponents of smart city technologies also worry that smart cities and communities will violate individuals' privacy by engaging in government surveillance.

This report explores the close and important relationship between smart cities and data privacy. It first explains the types of data smart city technologies collect, reasons for collecting this data, and the sensitivity of this data as it relates to residents' privacy. Next, it outlines and fact-checks the top privacy concerns associated with smart cities. It also presents other concerns smart cities and communities should consider along with privacy. Finally, it recommends solutions that balance and address these concerns, including:

- Congress should pass comprehensive federal data privacy legislation.
- State lawmakers should set rules on accountability and transparency for law enforcement use of smart city data, such as from surveillance cameras and gunshot detection technology.
- Cities and communities should anonymize stored personal data wherever possible.
- Cities and communities should not require third parties to turn over sensitive personal data about their users as a condition of operating there.

- Cities and communities should prioritize cybersecurity when implementing smart city technologies.
- Cities and communities should set and enforce privacy and cybersecurity rules for the private companies they partner with to provide smart city applications.

SMART CITIES AND DATA COLLECTION

There are many smart city technologies and applications that already exist and can serve as examples of the types of data collection that take place in a smart city or community. These examples are important for informing the debate around smart cities and privacy, as not all data collection poses an equal risk to individual privacy. The debate should focus on smart city technologies that collect sensitive data and could pose a serious risk to privacy if that data were misused or fell into the wrong hands.

Many smart city technologies do not collect any data on residents' behavior or activities, instead collecting data exclusively on the state of local infrastructure or the environment. Other technologies collect data not at an individual level but on residents' behavior collectively, so there is little to no privacy risk because doing so does not reveal anything about individuals. Another factor that weighs on the relative privacy risks associated with different smart city technologies is who has access to the collected data, including government entities, private companies, and individual residents. Data governments share more broadly may pose a greater risk than data that is only useful to the specific government entities involved in providing services to residents.

Smart Grid

Smart grid technologies are digital hardware and software embedded within the energy system, including smart meters, smart buildings, and smart appliances.[2] Smart meters provide real-time information on energy consumption and enable two-way communication between utilities and consumers. Smart appliances collect data on their energy performance and can be controlled remotely. And smart buildings gather data on energy use and other daily operations and then automate various processes.

These technologies enable two important energy-saving processes: dynamic pricing and demand response. Dynamic pricing is a rate structure in which utilities set variable prices for electricity that adjust in response to demand, as opposed to a flat per-kilowatt-hour rate. By charging higher rates during peak times, utilities can encourage consumers to reduce their demand temporarily by shifting non-time-sensitive demand to off-peak times when prices are low; this is demand response. A 2018 McKinsey report finds that dynamic pricing and demand response could cut emissions in smart cities by up to 5 percent.[3]

Smart grid technologies require real-time data on household and business energy use; the privacy implications of collecting this data are limited. In theory, someone with access to data on a household's energy use could roughly predict members' of that household's schedule, for nefarious reasons. It would therefore be important for utilities not to share household energy use data without first anonymizing it.

Smart Lighting

Smart lighting consists of Internet-connected LED street lighting that can be remote-controlled, monitored, and automated. Smart streetlights turn off and on or brighten and dim as needed in response to environmental factors and public safety concerns, leading to more efficient use of street lighting that could both save cities and communities money and reduce their emissions.

At a basic level, cities and communities could program smart streetlights to automatically turn off during the day and on at night or during thunderstorms or other weather events. In an area that does not see much activity at night, cities and communities could, to conserve energy, program streetlights to only turn on in response to pedestrian or vehicle activity. Cities and communities could program smart streetlights with special lighting patterns for traffic and crowd control and give first responders the ability to increase lighting to assist with their work.[4] Cities and communities could also increase lighting in high-crime areas as a potential deterrent.[5]

None of these use cases require sensitive or personal data from residents or extensive data sharing; however, because smart streetlights are conveniently located Internet-connected devices, they could also serve as Wi-Fi hotspots or provide a foundation for other smart city applications.[6] For example, cities or communities could attach closed-circuit TV (CCTV) cameras to smart streetlights to aid in solving crime.[7] While smart streetlights with cameras collect much more data than do streetlights without cameras—in the form of video footage shared with law enforcement when a crime occurs in an area—they are no more invasive than the many existing publicly and privately owned security cameras that monitor public places and have served as a useful tool for law enforcement for decades.[8]

Smart Trash Cans

Smart trash cans and recycling bins are equipped with sensors that alert sanitation departments when they need to be emptied, allowing these departments to plan more efficient schedules and routes and thereby save cities and communities time, money, and energy. Emptying public trash cans and recycling bins before they're full is unnecessary and a waste of resources: labor costs, fuel consumption, and wear and tear on vehicles. Waiting too long, on the other hand, leads trash cans and recycling bins to overflow, which is unsightly, unsanitary, and bad for the environment.[9] Litter also comes with costs, including an estimated $1.3 billion in annual cleanup costs to states, cities, and counties, according to a 2009 survey.[10]

The only data smart trash cans and recycling bins need to collect in order to function is the status of the cans and bins themselves. This does not involve any sensitive personal information—or, in fact, any personal information at all—leading to a negligible risk to individuals' privacy. Additionally, the data from smart trash cans is primarily useful to waste management services and should not require sharing outside of that context.

Like smart streetlights, smart trash cans and recycling bins serve as Wi-Fi hotspots or as a platform for other telecom and IT infrastructure.[11] However, they would not be as useful for certain smart city applications. Streetlights and trash cans are both conveniently located throughout cities, but streetlights have a higher vantage point that is more useful for CCTV cameras and gunshot detection sensors.

Smart Water Management

Smart water management systems consist of sensors in a city's or community's water pipelines that collect data on the conditions of the infrastructure and relevant weather activity. They can detect combined sewage overflows—overflows in sewers that collect rainwater runoff, domestic sewage, and industrial wastewater due to heavy rain—and track the levels of chemicals. By analyzing the data from these sensors, cities and communities can also predict when and where floods are likely to occur.[12]

Using smart water management systems, cities and communities can respond more quickly to leaks, overflows, and harmful levels of chemicals and prepare more effectively for floods. This could lead to less water wasted and improve the quality of drinking water, which will become increasingly important as climate change threatens both the availability and quality of water supplies in the United States and around the world. Climate change also leads to more frequent severe weather events, which results in more flooding.[13]

The data smart water management systems collects is not related to individual residents' behavior or activities, making it a very low risk to privacy. It also only needs to be accessible to government entities in charge of water management for the city or community. At the same time, smart water management systems have real benefits (e.g., Ann Arbor, Michigan, implemented a smart water management system called Open Storm to track storm water and saved $1 million in infrastructure costs).[14]

Environmental Monitoring Sensors

Another smart city application that allows cities and communities to predict potentially hazardous conditions is environmental monitoring sensors. These sensors monitor environmental conditions, including temperature, precipitation, humidity, wind, solar radiation, atmospheric pressure, and other factors.[15]

With constant, real-time data on environmental conditions, cities and communities can better inform their environmental policies, monitor air quality, predict weather events, and protect critical infrastructure. Cities and communities could choose to share the environmental data they collect with outside entities, such as utility companies that would use more accurate weather prediction to help reduce power outages, saving businesses and households money. A 2020 economic analysis for the American Society of Civil Engineers estimates the annual cost of power interruptions at $85 billion.[16]

Cities and communities could also develop websites or apps that would allow residents to access environmental data relevant to their day-to-day lives. And even though cities and communities might end up sharing environmental data widely, the risk to individual privacy would still be low, as such data does not include personal information on residents.

Intelligent Traffic Signals

There are many transportation-related smart city applications. For instance, intelligent traffic signals collect information on traffic conditions from roadway sensors, traffic cameras, connected vehicles, and other devices to adjust the timing of traffic lights and other signals. The goal is to reduce the amount of time people spend waiting at intersections, thereby reducing traffic.

This leads to multiple benefits. From an individual standpoint, drivers and riders spend less time in traffic. From an economic standpoint, commuters get to and from work more quickly and goods are delivered faster, resulting in increased productivity. Finally, from an environmental standpoint, vehicles waste less fuel idling at traffic lights, resulting in lower emissions. In 2021 in the United States, drivers lost an average of 36 hours to sitting in traffic and spent an average of $564, with much higher numbers—up to 102 hours and $1,595—in the most congested cities, according to an annual report by INRIX. The total economic cost of traffic congestion was an estimated $53 billion.[17]

Intelligent traffic signals need to gather data on traffic conditions, such as how many vehicles are on the road and where those vehicles are located. This could, therefore, include collection of location data from individual connected vehicles. As long as this data is only used for the purposes of adjusting traffic signals and reducing traffic and is not shared with outside entities, the risk to individual privacy is low. An additional step cities and communities should take to further reduce privacy risks is anonymizing the location data and deleting it when no longer useful.

Advanced Public Transportation

Another transportation application of smart city technology, advanced public transportation systems consist of public transit vehicles—such as buses and trains—that communicate with each other, sharing data on their location, arrival and departure status, and overall timeliness. These systems also communicate information to riders via a website or app and electronic signage at bus and train stations.

With advanced public transportation systems, smart cities and communities would have accurate, real-time information on the status of all public transportation assets, allowing for better decision-making that could decrease costs and increase efficiency. Riders could better plan their commute and reduce their "buffer time" (the amount of time they spend waiting for their bus or train to arrive). A 2015 McKinsey report estimates that up to 70 percent of the time people spend commuting is buffer time, and reducing that buffer time could lead to time savings of over $60 billion per year globally.[18]

Unlike intelligent traffic signals, advanced public transportation systems would not require any location data from privately owned vehicles; they would only need the location data of public transit vehicles, which does not pose a risk to individuals' privacy. Theoretically, an app that provides riders with real-time updates on public transportation could request users' location data for a more personalized experience, which would pose similar risks to any other website or mobile app that collects users' location data.

Smart Parking

Smart parking meters sense when and where parking spots are available in a city or community, and smart parking apps direct drivers to convenient parking spots near their destination. The goal of smart parking is to reduce the amount of time drivers spend searching for parking, which in turn saves drivers money on fuel and reduces emissions. By directing drivers to available parking spots, smart parking apps may also serve as a source of revenue for cities and communities that charge for parking.

Smart parking meters would only need to track the status of parking spots—whether a parking spot is occupied, and perhaps also how long it has been occupied—but the apps these meters communicate with would need more data. Unlike advanced public transportation apps, which may request users' location data but could still provide some function without location data, smart parking apps would need users' location data in order to direct users to nearby parking. Once again, this would only pose similar privacy risks to existing websites and mobile apps that collect users' location data.

Congestion Pricing

Cities around the world have engaged in congestion pricing—charging vehicles a fee for driving in congested areas during the busiest times of day—for decades.[19] The state of Virginia introduced a form of congestion pricing for drivers commuting alone to D.C. in 2017, and New York City began planning its own congestion pricing scheme in 2019.[20]

Congestion pricing generates revenue for state and local governments and incentivizes drivers to carpool, travel during non-peak times, or use alternative transportation options that have a lower environmental impact, such as public transportation, walking, or bicycling. The goal is to reduce traffic and emissions. By combining congestion pricing with smart city technology such as roadway sensors and connected vehicles, cities and communities can collect real-time data on traffic conditions and the number of vehicles on the road and adjust tolls accordingly.

Currently, many U.S. states use E-Z Pass to electronically collect tolls from toll roads, high-occupancy toll lanes—which exempt vehicles with a certain number of passengers from paying fees—and express lanes.[21] Electronic toll collection allows drivers to pay tolls automatically via a device or tag placed on their windshield. This requires municipalities to collect a limited amount of location data on individual vehicles, specifically data on when and where each vehicle paid an electronic toll. However, smart cities and communities could use systems that collect less data, such as road user charges, which charge users based on miles traveled via onboard units in each vehicle that only share information on how much the vehicle's driver owes, and not information on where or when the vehicle drove.[22] Alternatively, smart cities and communities could delete trip data after payment is processed.

Gunshot Detection

Gunshot detection involves sensors equipped with microphones, GPS, and cell service placed around an area to constantly record audio and monitor for the sound of gunshots and alert the police. ShotSpotter, a popular vendor for gunshot detection, has described in detail how the technology works. It places between 15 and 20 sensors per square mile at least 20 feet above the ground. When three or more sensors detect a possible gunshot, a central server sends the audio to a review center for analysis by a human, who then sends an alert along with the audio to the local police.[23]

The goal of gunshot detection is to reduce the amount of time it takes to dispatch officers to the scene of a shooting and, hopefully, in the long term, reduce gun violence. According to ShotSpotter, 80 percent of shootings are never reported to the police. Gunshot detection lowers the number of unreported shootings to below 10 percent. ShotSpotter also reports that it reduces the amount of time it takes to dispatch officers to the scene of a shooting from an average of 4.5 minutes to under 60 seconds.[24]

The potential privacy concern involving gunshot detection is sensors' collection of audio recordings. Without safeguards, microphones placed around a city could theoretically record conversations or other interactions. However, currently, gunshot detection is designed only to listen for explosive, gunshot-like sounds. ShotSpotter retains audio recordings for a limited amount of time in case of missed gunshots, after which sensors overwrite the old recordings with new ones.[25]

TOP PRIVACY CONCERNS

The technologies covered in this report are a general overview of the types of applications smart cities and communities have already begun to use, most of which pose a low risk to individual privacy. However, concerns around privacy in smart cities and communities are still a major topic of discussion and debate. This is in part due to legitimate risks that could result from mismanagement or a failure to prioritize data privacy and security, and in part due to fear over hypothetical future smart city applications and their uses and the exploitation of those fears by certain advocacy organizations.

Privacy concerns related to smart cities and communities tend to fall into three categories: data security, commercial use of data, and government surveillance.

Data Security

Security and privacy are closely related concerns. Entities that collect individuals' personal data have a responsibility to keep that data secure from unauthorized access. Data breaches can, and often do, result in individuals' personal data ending up in the wrong hands, including criminals and even foreign state-sponsored hacking groups. They also result in significant economic losses. The average cost of a public sector data breach in 2022 was just over $2 million.[26]

Smart cities and communities are especially vulnerable to cyberattacks because of their use of IoT devices, which are commonly targeted and frequently insecure, and present a large attack surface. The potential security risk of IoT devices has been well documented since their introduction, and many stakeholders and experts have called attention to the need for stronger security protections. These devices are often connected to the Internet, providing attackers with an entry point into other systems they are left unsecured.[27]

Another factor impacting governments' vulnerability to cyberattacks is the amount of data—particularly sensitive data—they collect on their employees and citizens, which is the case even without smart city data collection. Many large-scale cyberattacks target governments.[28] Governments also control critical infrastructure, another valuable target for attackers.

Finally, governments often fail to prioritize cybersecurity. Local governments in particular have limited budgets with which to procure secure technologies, regularly update those technologies, and hire and retain cybersecurity experts.[29] A survey of local government entities in the United States finds that nearly one-third would not even be able to detect having been hacked.[30] Governments at all levels also need to accelerate their transition to cloud computing, which, among other benefits, is more secure.[31]

All these factors combined make smart cities and communities an attractive target for cyberattacks. The number of entities that have access to that data can also increase

vulnerability; for example, if a smart city or community shares certain data with a private partner, a cyberattack on either the local government or the private partner could compromise that data.

Data security is a legitimate concern for smart cities and communities and should be a top priority. Effectively addressing this concern will require local governments to increase their investment in cybersecurity, follow cybersecurity best practices, update IT systems, require their private partners to follow the same practices, and exercise caution in procuring smart city technologies.

Commercial Use of Data

The second category of common privacy concerns related to smart cities and communities is the commercial use of smart city data. There are two ways this could take place. First, a city or community could partner with a private company to pay for or provide certain smart city technologies and in return give the company access to the data the city or community collects. Second, a city or community could sell localized advertisements that do not target individual residents personally but instead target the broader community.

In the first scenario, the privacy concern arises if a city or community shares residents' sensitive personal data with private partners, particularly if there are no rules or restrictions on how those private partners can use that data, the data collection and sharing is not transparent for residents, and residents have no opportunity to give or revoke consent for data sharing. To better protect residents' privacy when sharing their data, smart cities and communities can set rules for their private partners' use of smart city data, and follow up to ensure continual compliance. Federal privacy legislation that creates rules for all commercial use of personal data would go a long way toward regulating these activities across the board. De-identifying residents' data would also minimize the privacy risks of commercial data sharing.

In the second scenario, cities and communities have no need to share residents' personal data with advertisers. Unlike targeted advertisements, which target consumers online based on their individual traits and shopping or browsing history, localized advertisements target the entire community. For example, Boston-based start-up Soofa creates solar-powered digital signs that display information on local news, events, public transit, and more. Communities can finance these signs by displaying ads from local businesses.[32]

Theoretically, smart cities and communities could also sell targeted advertisements if they collected enough personal data from residents. This would still not necessitate cities and communities to share this data directly with advertisers. The way most targeted ads work online is an ad network collects data on users and then charges advertisers to target certain audiences.[33] The ad network does not actually share user data with the advertisers. Smart cities and communities could operate in a similar fashion, selling advertisers the opportunity to target ads to certain audiences.

Smart cities and communities taking this approach would still likely face opposition because of widespread misinformation about how targeted advertising works. But cities and communities need to fund their smart city initiatives somehow. There are other ways besides selling targeted ads, including the aforementioned public-private partnerships, as well as federal government grants, raising taxes, collecting tolls, or charging user fees. Some of these funding sources could involve fewer privacy trade-offs for residents, but they also may be less accessible for all cities

and communities (in the case of grants) or more expensive for residents (in the case of taxes, tolls, and fees). Each city and community will need to weigh the pros and cons of different funding sources.

Case Study: Sidewalk Toronto

Sidewalk Toronto was a proposed smart city partnership between Toronto, Canada, and Sidewalk Labs, a subsidiary of Alphabet. The partnership, proposed in 2017, would develop Toronto's waterfront Quayside area—including by building up the area's digital infrastructure and providing smart city applications in areas such as traffic, waste, water, and energy management—with the opportunity for Sidewalk Labs or other entities to provide additional applications in the future.[34]

Sidewalk Labs' proposal resulted from 18 months of public engagement with more than 21,000 Torontonians, but still faced opposition from privacy fundamentalists and was ultimately canceled in 2020 due to budgetary concerns arising from the COVID-19 pandemic.[35]

The opposition to Sidewalk Toronto reflects the ongoing "techlash," or backlash against Big Tech, as much of it was a result of Sidewalk Labs' proximity to Google, another Alphabet company.[36] Opposition did not subside when Sidewalk Labs responded to criticism, for example, committing to not selling residents' personal information to third parties or using it for advertising. It also responded to concerns over the potential for de-identified personal data to be re-identified by planning to have trusted external experts regularly attempt to re-identify the data.[37]

Government Surveillance

The final category of concerns related to smart cities and communities is the fear that governments will use smart city initiatives to surveil individuals, such as by gaining access to data they could not otherwise compel access to or building profiles of residents' behavior using data from a variety of different sources.

Critics of smart cities point out that, while much of the data smart city technologies collect poses a low risk to individual privacy on its own, it is theoretically possible for governments with access to enough data collected by smart city technologies to build detailed profiles of residents' behavior.[38] A pervasive narrative fuels these concerns: the myth that the Chinese Communist Party (CCP) uses artificial intelligence to monitor citizens' behavior and rank them using a "social credit" system that scores how "trustworthy" citizens are based on a variety of factors, including their spending habits, online activity, and rule-breaking behaviors. In reality, there is no high-tech, country-wide social scoring system in China.[39]

Additionally, the United States has many laws, including those enumerated in the Constitution and Bill of Rights, that restrict governments at every level from engaging in this type of surveillance. The worst-case scenario privacy fundamentalists envision would require the United States to stop functioning as a democracy and instead function as a totalitarian regime such as the CCP.

It is more likely that only certain governments might compel access to certain types of data. For example, the Los Angeles Department of Transportation requires operators of shared bikes and scooters to share location data on every trip taken, with only a five-second delay—a rule developed in anticipation of a future in which all vehicles will be fully autonomous and need to

communicate their location to each other to avoid collisions.[40] Critics have responded by arguing that requiring this amount of detailed, nearly real-time, individual-level data sharing is an unnecessary violation of privacy.[41] Cases regarding this type of compelled access to data may end up in the courts, which will determine whether they violate existing privacy laws or even the Fourth Amendment.

BALANCING PRIVACY AGAINST OTHER CONCERNS

Cities and communities should take their residents' privacy into account when implementing smart city technologies, but this should not be their only priority. If privacy were governments' only priority, governments would never collect data on their citizens; but governments do because there are legitimate reasons why they may need this data. Likewise, there are a number of other concerns cities and communities need to balance against privacy, including public safety, sustainability, beneficial uses of data, and cost.

Public Safety

First, balancing privacy and public safety is a common trade-off governments have to make. Gunshot detection is a prime example of this in smart cities and communities. While it can have many benefits, enabling law enforcement to respond quickly to potential shootings, some privacy fundamentalists oppose the use of gunshot detection because governments could theoretically use the sensors to listen in on residents' conversations.[42] Similar concerns abound in the world of police technology: On the one side, law enforcement and public safety advocates argue that new technologies can save lives, and on the other side, privacy and civil rights advocates argue that these technologies could enable law enforcement to infringe on Americans' rights.[43]

Balancing privacy and public safety involves setting boundaries around the use of certain technologies that limit the potential for harm without banning law enforcement from using new tech. In the case of gunshot detection, many of the policies ShotSpotter already follows serve as good examples of boundaries designed to prevent misuse. The sensors only send audio to a review center if they detect a potential gunshot, and then human reviewers only forward that audio to the police if they confirm that the audio is likely a gunshot. Furthermore, audio is automatically overwritten after a certain period of time, so law enforcement cannot dig up old recordings to listen in on captured conversations or other audio.

There are always risks associated with new technologies, but especially when the potential benefit is more lives saved, it is crucial for cities and communities to weigh the risks and benefits. Privacy fundamentalists will continue to advocate for bans of any potentially risky technology, and may succeed in some cases.[44] But the cities and communities that balance both public safety and privacy, instead of sacrificing one in favor of the other, will reap the benefits of new and emerging technologies and lead the way in smart city adoption, while cities and communities that resort to bans will miss out and fall behind.

Sustainability

Another key consideration for smart city technologies is their potential to lower cities and communities' environmental impact.[45] Energy-related applications such as smart lighting and the smart grid can help cities and communities use less electricity, waste management applications can help cities cut back on litter, and transportation applications such as intelligent traffic signals, smart parking, and congestion pricing can reduce emissions from vehicles. These

and other technologies will be an important tool in cities' and communities' tool kits as local leaders increasingly prioritize sustainability, such as the 470 U.S. mayors who have pledged to take action on climate change through the Climate Mayors network.[46]

The potential trade-offs between sustainability and privacy are a classic example of the trade-offs between collective and individual benefit. Climate change is a collective problem. It requires many actors—individuals, companies, and governments—to take many different actions to reduce their environmental impact. If individuals, companies, and governments are successful at addressing climate change, everyone will reap the benefits.

Privacy, on the other hand, is an individual concern. Every individual has a right to privacy, but when data sharing can result in positive externalities for the collective—such as increased sustainability and reduced environmental impact—it is important to weigh both. Meaningful climate action should not require governments to seriously infringe on individual privacy, particularly in ways that cause actual harm. But since data collection and sharing can help sustainability efforts, casting all data collection and sharing in a negative light (as some privacy fundamentalists do) will impede climate progress.

Beneficial Uses of Data

There are many other beneficial uses of data besides public safety and sustainability. For example, data collection and sharing can bolster public health by helping researchers track, prevent, and cure disease and city and community officials create better policies.

Many countries, states, cities, and communities used contact tracing apps, which identify and notify individuals who have been in close contact with individuals who tested positive for COVID-19. These apps required users' location data, and users had to download them and opt in to sharing their data, which resulted in fewer people participating in digital contact tracing than was necessary to effectively reduce cases of COVID-19 in many places. One study from 2021 finds that individual privacy concerns were a significant reason behind many peoples' reluctance to download contact tracing apps.[47]

This is another example of the trade-offs between collective and individual benefit. Effective contact tracing can lower the number of infections and mortality rate from COVID-19, which is a significant benefit to society.[48] But many people weighed the risk to their individual privacy posed by sharing their location data as higher than the risk to those around them who they could unknowingly infect with COVID-19.

Smart cities and communities need to weigh the beneficial uses of data against the risk to individual privacy. There are many ways to accomplish this, such as setting higher privacy standards for sensitive data than nonsensitive data, setting fewer restrictions on using and sharing anonymized data, and providing individuals with transparency into how their data is used and shared.

Cost

The final consideration, a factor every government has to take into account, is cost. Smart city technologies can lead to cost savings over time through increased efficiency and productivity, but governments still have to bear the up-front costs of procuring and installing these technologies, as well as recurring maintenance costs. For example, data from 2010 reveals that the average

cost of installing "adaptive traffic control systems" (i.e., intelligent traffic signals) in the United States was $65,000 per intersection.[49] This was a significant cost, particularly for smaller cities and communities with more limited budgets, and only represents one smart city application.

To offset the costs of implementing smart city technologies, some cities and communities rely on private partners. For example, Kansas City partnered with Cisco and Sprint in 2014 to install 25 free public Wi-Fi and interactive kiosks along the city's streetcar route. The government of Kansas City spent $3.7 million on the project while Cisco and Sprint spent $12.3 million, covering the majority of the cost. In return, the companies had exclusive access to the Wi-Fi usage data from the kiosks.[50]

Privacy fundamentalists often oppose these types of public-private partnerships in smart cities and communities, citing concerns over how companies will use the data they gain access to. Toronto's smart city partnership with Sidewalk Labs faced this kind of opposition, including a successful lawsuit by the Canadian Civil Liberties Association.[51]

Cities and communities can also obtain funding for smart city initiatives in the form of government grants—but there is not enough federal funding for every city and community in America. Meanwhile, raising taxes in order to fund smart city initiatives could lead to just as much backlash from residents who do not want to pay higher taxes. Realistically, many cities and communities will need to rely on private partners.

There are plenty of ways for these cities and communities to protect their residents' privacy while partnering up with companies. Smart cities and communities should require their private partners to follow data privacy and security standards designed to prevent data breaches and misuse of sensitive personal data. Smart cities and communities should also maintain oversight over their private partners to ensure those partners are adhering to the standards set for them.

RECOMMENDATIONS

Even while taking competing concerns into account, there are several steps federal, state, and local governments can take to preserve individual privacy without impeding cities' and communities' ability to experiment with smart city technologies.

To address concerns about security:

- Cities and communities should prioritize cybersecurity when implementing smart city technologies, such as by setting high security requirements for procuring Internet-connected devices, encrypting smart city data, implementing network access controls and monitoring, conducting regular threat and risk assessments, and transitioning to cloud computing.
- Cities and communities should engage in vendor management when partnering with private companies to provide smart city applications. This entails requiring cities' and communities' private partners follow privacy and security standards and only use the data they have access to for predetermined purposes. Cities and communities should conduct regular audits of their private partners to ensure they adhere to these standards.

To address concerns about commercial use of data:

- Congress should pass comprehensive federal data privacy legislation that preempts existing state and local laws and protects all Americans while allowing room for data-

driven innovation, including smart city applications.[52] This should include opt-in consent for commercial use of sensitive data, opt-out consent for commercial use of nonsensitive data, and transparency requirements that provide individuals with basic information on how their data is collected and used.

To address concerns about government surveillance:

- State lawmakers should regulate law enforcement data collection, including limiting the amount of time law enforcement agencies can retain data that is not potential evidence for a crime, only allowing the collection of sensitive data for specific purposes related to solving or responding to crime, and requiring transparency around how police use, store, and protect individuals' personal data.[53]
- As much as is possible, cities and communities should anonymize any personal data they collect via smart city technologies to reduce the potential threat to individuals' privacy. Where possible, cities and communities should also delete stored personal data after a certain period of time when the data is no longer useful for its intended function.
- Cities and communities should not require third parties to turn over sensitive personal data about their users as a condition of operating in the city, but could require sharing of anonymized or other nonsensitive data.

About the Author

Ashley Johnson (@ashleyjnsn) is a senior policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation, and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit us at itif.org.

ENDNOTES

1. Colin Cunliff, Ashley Johnson, and Hodan Omaar, "How Congress and the Biden Administration Could Jumpstart Smart Cities With AI" (ITIF, March 2021), https://www2.itif.org/2021-smart-cities-ai.pdf.
2. Ibid.
3. McKinsey Global Institute, "Smart Cities: Digital Solutions for a More Livable Future" (McKinsey & Company, June 2018), https://smartcitiesoftheworld.com/2023/01/23/smart-cities-digital-solutions-for-a-more-livable-future/.
4. Remy Marcotorchino, "Connected Street Lighting: A Strong Foundation for a Smart City," *IIoT World*, June 12, 2018, https://iiot-world.com/smart-cities-buildings-infrastructure/smart-cities/connected-street-lighting-a-strong-foundation-for-a-smart-city/.
5. Aaron Chalfin et al., "Reducing Crime Through Environmental Design: Evidence From a Randomized Experiment of Street Lighting in New York City" (National Bureau of Economic Research, May 2019), https://www.nber.org/system/files/working_papers/w25798/w25798.pdf.
6. Marcotorchino, "Connected Street Lighting."
7. Ashley Johnson, Eric Egan, and Juan Londoño, "Police Tech: Exploring the Opportunities and Fact-Checking the Criticism" (ITIF, January 2023), https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/.
8. "The Evolution of Closed-Circuit Television (CCTV) Systems," Vector Security Networks, updated January 20, 2021, https://vectorsecuritynetworks.com/the-evolution-of-closed-circuit-television-cctv-systems/; Eric Piza, Joel M. Caplan, and Leslie W. Kennedy, "CCTV as a Tool for Early Police Intervention: Preliminary Lessons from Nine Case Studies," *Security Journal* 30, no.1 (2016): 247–265, https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1185&context=jj_pubs.
9. Global Industrial, "3 ways smart trash cans help cities streamline operations," *Waste Dive*, October 25, 2021, https://www.wastedive.com/spons/3-ways-smart-trash-cans-help-cities-streamline-operations/607748/; "How Does Littering Affect the Environment?" Texas Disposal Systems, May 4, 2020, https://www.texasdisposal.com/blog/the-real-cost-of-littering/.
10. MidAtlantic Solid Waste Consultants, *2009 National Visible Litter Survey and Litter Cost Study* (Keep America Beautiful, Inc., September 2009), https://kab.org/wp-content/uploads/2019/08/News-Info_Research_2009_NationalVisibleLitterSurveyandCostStudy_Final.pdf.
11. "ICT Hosting Platform," Bigbelly, accessed December 8, 2022, https://bigbelly.com/products/telebelly/.
12. Naveen Joshi, "Smart wastewater management systems in smart cities," Allerin, January 18, 2020, https://www.allerin.com/blog/smart-wastewater-management-systems-in-smart-cities.
13. Upmanu Lall et al., "Water," in *Impacts, Risks, and Adaptations in the United States: Fourth National Climate Assessment, Volume II*, edited by David Reidmiller et al. (Washington, D.C.: U.S. Global Change Research Project, 2018): 145–173, https://nca2018.globalchange.gov/downloads/NCA4_2018_FullReport.pdf.
14. Mickey McCarter, "Smart Cities Connect 2018: How Ann Arbor (Mich.) Drained Stormy Waters Smartly," *StateTech*, March 29, 2018, https://statetechmagazine.com/article/2018/03/smart-cities-connect-2018-how-ann-arbor-mich-drained-stormy-waters-smartly.
15. Bacco Manlio et al., "Environmental Monitoring for Smart Cities," *IEEE Sensors Journal* 17, no. 23 (2017): 7767–7774, https://arxiv.org/pdf/2205.15147.pdf.
16. EPB US, "Failure to Act: Electric Infrastructure Investment Gaps in a Rapidly Changing Environment" (American Society of Civil Engineers, 2020),

https://www.asce.org/uploadedFiles/Issues_and_Advocacy/Infrastructure/Content_Pieces/failure-toact-electricity-report.pdf.

17. Bob Pishue, "2021 INRIX Global Traffic Scorecard" (INRIX, December 2021).
18. James Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype" (McKinsey Global Institute, June 2015), https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20internet%20of%20things%20the%20value%20of%20digitizing%20the%20physical%20world/unlocking_the_potential_of_the_internet_of_things_executive_summary.pdf.
19. Hannah Parks, "Investigating the Impact of Congestion Pricing Around the World," Climate Xchange, March 29, 2019, https://climate-xchange.org/2019/05/29/investigating-the-impact-of-congestion-pricing-around-the-world/.
20. Aarian Marshall, "Virginia's $40 Toll Road Better Be the Future of Driving," *Wired*, December 9, 2017, https://www.wired.com/story/virginia-i66-toll-road/; Associated Press, "NYC Moving Ahead With Congestion Pricing Toll Plan: Here's What It Looks Like," *NBC New York*, August 24, 2022, https://www.nbcnewyork.com/news/local/new-york-city-moving-ahead-with-congestion-pricing-toll-plan/3798060/.
21. "About E-Z Pass: Where can I use it?" E-Z Pass, accessed December 13, 2022, https://www.e-zpassiag.com/about-e-zpass/where-can-i-use-it.
22. Robert D. Atkinson, "The Best Way to Fund the U.S. Surface Transportation System," *Morning Consult*, July 26, 2019, https://morningconsult.com/opinions/the-best-way-to-fund-the-u-s-surface-transportation-system/.
23. Jay Stanley, "Shotspotter CEO Answers Questions on Gunshot Detectors in Cities," ACLU, May 5, 2015, https://www.aclu.org/news/privacy-technology/shotspotter-ceo-answers-questions-gunshot.
24. "Gunshot Detection," ShotSpotter, accessed December 8, 2022, https://www.shotspotter.com/law-enforcement/gunshot-detection-technology/.
25. Stanley, "Shotspotter CEO Answers Questions."
26. "Cost of a Data Breach Report 2022" (IBM, July 2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.
27. Daniel Castro, "How Congress can fix 'internet of things' security," *The Hill*, October 28, 2016, https://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security/; James Andrew Lewis, "Managing Risk for the Internet of Things" (Center for Strategic & International Studies, February 2016), https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160217_Lewis_ManagingRiskIoT_Web_Redated.pdf; Aden Klein, "Biden Took the First Step on National Cybersecurity Standards. Congress Needs to Follow Through," New America, July 7, 2021, https://www.newamerica.org/oti/blog/biden-took-the-first-step-on-national-cybersecurity-standards-congress-needs-to-follow-through/; Joseph Lorenzo Hall et al., "Comments to the CPSC on the Internet of Things and Consumer Product Hazards," Center for Democracy and Technology, June 15, 2018, https://cdt.org/wp-content/uploads/2018/06/CDT-CPSC-IoT-Comments-061518.pdf.
28. "Significant Cyber Incidents," Center for Strategic & International Studies, accessed December 13, 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
29. Diana Baker Freeman, "Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It," *Governing*, May 6, 2022, https://www.governing.com/sponsored/why-local-governments-are-a-target-for-cyber-attacks-and-steps-to-prevent-it.

30. Richard Forno, "Local governments are attractive targets for hackers and are ill-prepared," Center for Internet and Society, March 28, 2022, https://cyberlaw.stanford.edu/blog/2022/03/local-governments-are-attractive-targets-hackers-and-are-ill-prepared.
31. Michael McLaughlin, "Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services" (ITIF, June 2020), https://www2.itif.org/2020-fedramp.pdf; Meghan Sullivan, Malcolm Jackson, Joe Mariani, Pankaj Kamleshkumar Kishnani, "Don't just adopt cloud computing, adapt to it," Deloitte, January 21, 2022, https://www2.deloitte.com/us/en/insights/industry/public-sector/public-sector-cloud-adoption.html.
32. Kristin Musulin, "How Soofa helps shape the future of sustainable ad-funded infrastructure," *Smart Cities Dive*, December 13, 2018, https://www.smartcitiesdive.com/news/soofa-sustainable-ad-funded-infrastructure/544137/.
33. "How Do Online Ads Work?" (ITIF, November 2021), https://www2.itif.org/2021-online-advertising.pdf.
34. "Sidewalk Toronto," Sidewalk Labs, accessed February 8, 2023, https://www.sidewalklabs.com/toronto.
35. Moira Warburton, "Alphabet's Sidewalk Labs cancels Toronto 'smart city' project," *Reuters*, May 7, 2020, https://www.reuters.com/article/us-canada-sidewalk/alphabets-sidewalk-labs-cancels-toronto-smart-city-project-idUSKBN22J2FN.
36. Robert D. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress" (ITIF, October 2019), https://www2.itif.org/2019-policymakers-guide-techlash.pdf.
37. "Sidewalk Toronto," Sidewalk Labs.
38. Maya Shwayder, "The future of smart cities may mean the death of privacy," *Digital Trends*, April 22, 2020, https://www.digitaltrends.com/news/smart-cities-privacy-security/.
39. Melissa Heikkilä, "The AI myth Western lawmakers get wrong," *MIT Technology Review*, November 29, 2022, https://www.technologyreview.com/2022/11/29/1063777/the-ai-myth-western-lawmakers-get-wrong/.
40. Laura Bliss, "This City Was Sick of Tech Disruptors. So It Decided to Become One," *Bloomberg*, February 21, 2020, https://www.bloomberg.com/news/articles/2020-02-21/as-l-a-plays-tech-disruptor-uber-fights-back.
41. Jamie Williams, "Unchecked Smart Cities are Surveillance Cities. What We Need are Smart Enough Cities," Electronic Frontier Foundation, March 18, 2020, https://www.eff.org/deeplinks/2020/03/unchecked-smart-cities-are-surveillance-cities-what-we-need-are-smart-enough.
42. "Acoustic Gunshot Detection," Electronic Frontier Foundation, accessed October 20, 2022, https://www.eff.org/pages/gunshot-detection.
43. Johnson, Egan, and Londoño, "Police Tech."
44. David Lee, "San Francisco is first US city to ban facial recognition," *BBC*, May 15, 2019, https://www.bbc.com/news/technology-48276660; Rachel Metz, "Portland passes broadest facial recognition ban in the US," *CNN*, September 9, 2020, https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.
45. Cunliff, Johnson, and Omaar, "How Congress and the Biden Administration."
46. "Climate Mayors," Climate Mayors, accessed December 15, 2022, https://climatemayors.org/.
47. Eugene Y. Chan and Najam U. Saqib, "Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high," *Computers in Human Behavior* 119 (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7840411/.

48. Kevin Jenniskens et al., "Effectiveness of contact tracing apps for SARS-CoV-2: a rapid systematic review," *BMJ Open* 11, no.7 (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8277487/.
49. National Academies of Sciences, Engineering, and Medicine, "Implementation Costs and Benefits," in *Adaptive Traffic Control Systems: Domestic and Foreign State of Practice* (Washington, D.C.: The National Academies Press), 36-42.
50. John Skowron, Michael Flynn, and Tiffany Fishman, "Using public-private partnerships to advance smart cities" (Deloitte, 2018), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-public-private-partnerships-smart-cities-funding-finance.pdf.
51. Warburton, "Alphabet's Sidewalk Labs."
52. Johnson and Castro, "Maintaining a Light-Touch Approach."
53. Johnson, Egan, and Londoño, "Police Tech."