March 2021

IoT Strategy

The New York City Internet of Things Strategy

NYC Mayor's Office of the Chief Technology Officer

nyc.gov/cto

First published

March 4th, 2021

Version

File version 1.26.0402

Type

Typeset in *Libre Baskerville* and *Public Sans*, with accents of *Space Mono*.

Online

nyc.gov/cto

nyc.gov/assets/cto/#/project/iot-strategy

Acknowledgments

The NYC IoT Strategy builds upon research and publications prepared by former colleagues in the Mayor's Office of the Chief Technology Officer. NYC CTO would like to acknowledge their contributions, and to recognize the agency partners and diverse range of stakeholders who shared their expertise and perspectives in the development of this document.

Note

The NYC IoT Strategy is subject to applicable laws, rules, and regulations, including City procurement rules and processes. The City reserves all rights, including rights to postpone, cancel, or amend the IoT Strategy at any time. The City shall not be liable for any costs incurred in connection with the IoT Strategy.

Message from the CTO

Each decade brings change. Often, that includes the introduction of new technologies into our lives and lexicons.

The 2020s will be a critical decade for the billions of internet-connected devices commonly known as the Internet of Things, or “IoT” for short. Smarter homes, smarter services, and smarter cities. These advances – ranging from wearable health bands to self-monitoring factory equipment to pedestrian counters in parks – bring the potential for new jobs, a higher quality of life, and a climate-friendlier Big Apple. In this decade, society is poised to unlock these and countless other benefits from IoT. It is in this decade, too, that the rules of the road will be set, which is why now is the right time for us to face hard questions about the data economy, data poverty, digital rights, and potential deleterious uses of IoT.

The publication of the *New York City Internet of Things Strategy* fulfills the Mayor’s commitment in OneNYC 2050 by providing an update on the current IoT landscape and a bold vision for the future. New York City can and should lead the way. The following pages show how.

Technology, at its best, is a powerful force for good. The printing press helped humankind retain knowledge over generations. Photography allowed families to keep lasting images of their loved ones. The internet has enabled millions of students to learn safely during a global pandemic. Of course, these technologies didn’t decide their own futures… people did. Now, it is our turn – those of us in government, academia, non-profits, the private sector, and community-based organizations – to shape the future of the Internet of Things. We hope you’ll join us in this important effort.

Sincerely,

John Paul Farmer

John Paul Farmer

Chief Technology Officer,
The City of New York

Table of Contents

The Landscape

The Strategy

Executive Summary

Use of the Internet of Things ("IoT") is growing rapidly around the world, with applications proliferating across sectors and impacts being felt across society. From consumer "smart home" and "wearable" technologies, to retail and industrial IoT, to "smart city" applications, the world is seeing these "connected" technologies grow year over year in both volume and variety. New York City is no exception. The city has been home to a major expansion in IoT use in the last decade, with impacts on its transportation, utility services, resiliency, health, safety, and quality of life, among other areas.

IoT presents tremendous opportunity for New York. It can make our city and our lives more efficient, responsive, sustainable, convenient, and safe. But in order to produce these benefits and ensure they are equitably enjoyed, action is required.

The NYC IoT Strategy describes the landscape of IoT usage across society. It explores treatments of the technology in educational and policy settings. It outlines the state of New York City's IoT ecosystem. And it establishes a set of critical near-term actions toward creating a healthy, cross-sector IoT ecosystem in New York City – one that is productive, responsible, and fair.

The NYC IoT Strategy is built around six key principles:

- → Governance + Coordination
- → Privacy + Transparency
- → Security + Safety
- → Fairness + Equity
- → Efficiency + Sustainability
- → Openness + Public Engagement

These principles structure the City's approach, acting as guideposts for the analysis, recommendations, and actions set forth in this document.

Today, New York City faces a range of opportunities and challenges in fostering a healthy IoT ecosystem. Within City government, there are opportunities to build capacity to use and innovate with IoT, foster collaboration among agencies, boost partnership opportunities across sectors, and strengthen governance and coordination throughout the City. In the private and non-profit sectors, there are opportunities to support industry standards and best practices around IoT, coordinate on emerging workforce and IoT literacy needs, and support local economies and communities. In addition, there are opportunities to engage and empower residents in their interactions with IoT across society, as consumers, residents, or workers

The NYC IoT Strategy offers recommendations to address these issues and outlines five broad goals for near-term City action:

→ **Foster Innovation** by creating structures and programs that support research, testing, and experimentation with IoT technologies

→ **Promote Data Sharing and Transparency** around City IoT use by engaging residents about IoT initiatives, and aggregating information and data from the City's work to make them available across agencies, and for the public, where appropriate

→ **Improve Governance and Coordination** of the City's use of connected technologies through new policies and processes

→ **Derive Value from Cross-Sector Partnerships** by supporting and pursuing new opportunities for collaboration

→ **Engage with Industry and Advocate for Communities** by creating new channels for exchange and advocating for digital rights

By taking these steps, the City can advance toward a connected New York that works for all.

Introduction

Over the last decade, the use of internet-connected smart devices, or Internet of Things ("IoT") technology has grown across the globe. The number of connected devices worldwide is estimated to be in the tens of billions.[001] Uses of IoT run the gamut from consumer wearables and "smart home" products, to industrial and agricultural control systems, to "smart city" infrastructure. Year over year, the technology is expanding to new areas and applications at a rapid pace.

The term "IoT" describes the use of sensors or other electronic devices that collect data about the physical world and transmit their information, via the internet. The data that IoT or "connected" devices collect can be used independently – to inform operational or design decisions, for example. Or they can be used to communicate with other devices or systems to control conditions on the ground. A simple example would be a thermometer that reports its temperature reading to the Internet in order to help a city worker measure whether newly planted trees are cooling a street as intended, or to automatically shut off equipment in a factory when the temperature becomes too hot.

IoT technology is being used today in a range of sectors, affecting government, businesses, community groups, and residents. The technology presents tremendous opportunity for New York City. IoT can help government to improve planning and public safety, streamline operations, reduce costs, increase resiliency, improve sustainability, and respond to community needs. It can help local businesses and community organizations justify investment, optimize operations, and tailor products and services. It can improve New Yorkers' health, safety, opportunity, and overall quality of life.

In order to produce these benefits and ensure they are equitably enjoyed, there must be knowledge and capacity in place across society to understand and use the technology appropriately. There must be thoughtful planning and governance. And there must be transparency and engagement with those affected by IoT use to ensure buy-in and trust.

The Mayor's Office of the Chief Technology Officer has developed the NYC Internet of Things Strategy in order to support a healthy cross-sector IoT ecosystem in New York City – one that is productive, responsible, and fair.

[FIGURE 01 ▲] A view of New York City from a roof equipped with solar panels. *Photo: Mayoral Photo Office*

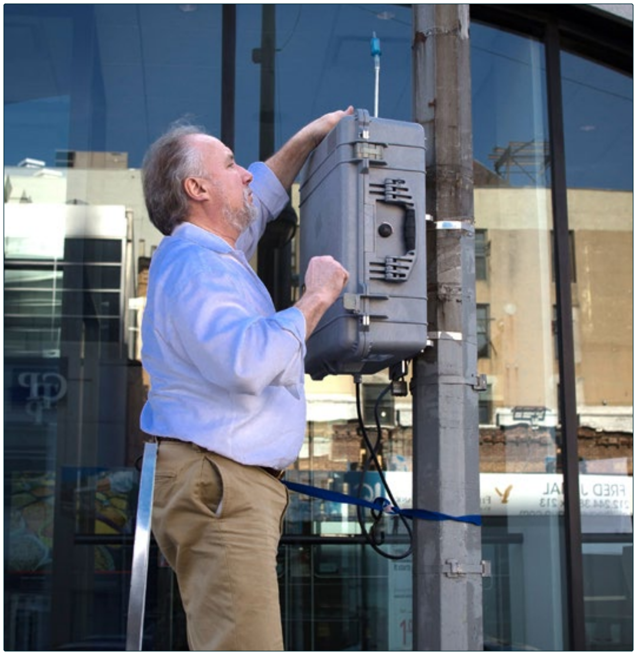
Foundational City Work

Over the last decade, New York City government has increased its use of connected devices to manage operations and infrastructure, and to provide services. As part of a broader set of efforts being undertaken to create what is often referred to as a "smart city," use of IoT in City government has, to date, largely been carried out by individual agencies, as specific opportunities to improve operations or projects have emerged.[002] Recognizing the potential that IoT presents, the need for greater awareness of its capabilities across City government, and the need for standards and governance for its use, the Mayor's Office of the Chief Technology Officer (NYC CTO) launched a set of efforts to organize the City's approach to IoT.

In 2015, NYC CTO published a foundational report, entitled "Building a Smart + Equitable City," featuring ten case studies across seven City agencies that "demonstrate the diversity of ways that connected technologies can help improve government services and better the lives of all New Yorkers."[003] This document was the first to highlight IoT projects undertaken by the City, and illustrated the operational and service improvements that could be possible when City agencies embrace connected technology.

In 2016, NYC CTO developed a "framework to help government and our partners responsibly deploy connected devices and IoT technologies in a coordinated and consistent manner."[004] Through wide-ranging engagements with stakeholders from the public sector, private sector, and academia, as well as a survey of government agencies across the world, NYC CTO identified more than 450 best practices for IoT use. These findings were distilled into a set of "Guidelines for the Internet of Things" for New York City to follow. These Guidelines have provided a foundation for the IoT initiatives New York City has in place today, and for the updated principles and recommendations outlined in the NYC IoT Strategy.

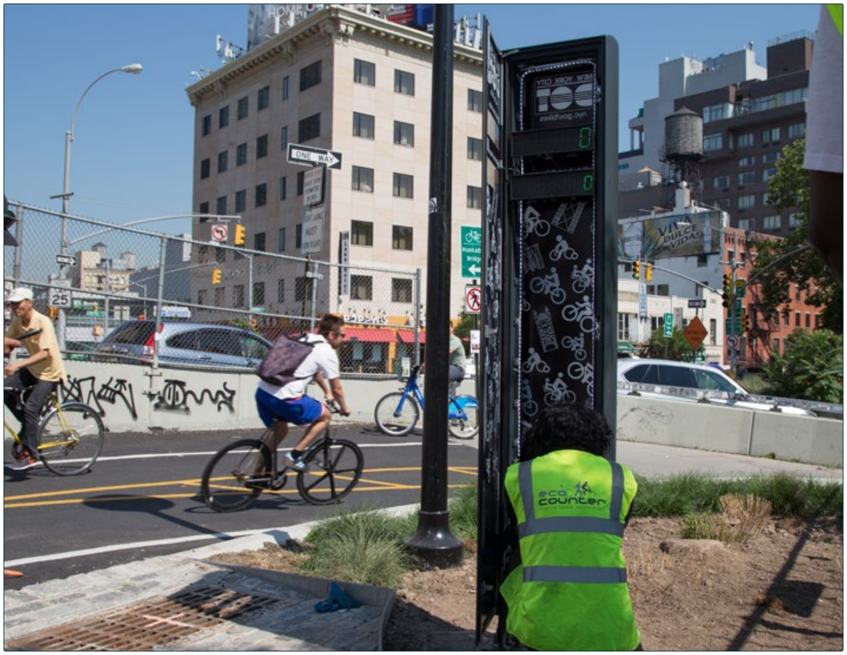
Since 2018, NYC CTO has partnered with City agencies to implement an array of pilot projects, initiatives, and stakeholder engagements that have also informed the IoT Strategy. These activities have included inter-agency working groups, an IoT device inventory, a



data dashboard prototype, and a range of exploratory data collection efforts. This work has provided important insights into gaps in the City's approach, as well as what might be possible with more coordinated and strategic effort.

Finally, in 2019, Mayor Bill de Blasio released his *OneNYC 2050* plan, outlining a broad vision for the future of New York City. As part of a set of commitments for "Modern Infrastructure," the City pledged to "centralize its approach to internet-connected sensing" via a formal Internet of Things strategy. The NYC IoT Strategy realizes the Mayor's commitment.

In developing this work, NYC CTO performed an updated review of government IoT plans and industry literature. In addition, NYC CTO engaged in conversations with stakeholder organizations across sectors, as well as agencies across New York City government, in order to present an up-to-date picture of governmental efforts, the state of New York City's IoT ecosystem today, and the particular opportunities and challenges New York City faces.



[FIGURE 02 ◀◀] A Department of Health and Mental Hygiene/Queens College air quality sensor being installed on a City street pole. *Photo: DOHMH*

[FIGURE 03 ◀] A bike counter being installed near the Manhattan Bridge by NYC Department of Transportation. *Photo: DOT*

IoT Principles

NYC CTO’s 2016 “Guidelines for the Internet of Things” underpin the City’s approach to using IoT in its own programs and operations. The NYC IoT Strategy broadens the City’s approach by providing a framework for stakeholders across government, industry, community groups, and city residents to consider what is necessary for a healthy IoT ecosystem – one that is productive, responsible, and fair. This framework is based on six key principles. These principles reflect the City’s broader commitment to digital rights for all New Yorkers.[005]

It is important to note that the IoT principles outlined here can sit in tension with one other. In any given product or project, decisions may need to be made about which specific principles or considerations ought to take precedence.

Governance + Coordination

IoT technologies and systems should be thoughtfully designed and deployed to ensure efficacy and viability through the life of the project or product.

Entities should perform ongoing oversight to ensure responsible and fair use, and account for emerging opportunities and risks.

Entities should optimize opportunities to coordinate IoT efforts to ensure interoperability and efficiency, and to maximize impact

Privacy + Transparency

IoT technologies and systems should protect and respect the privacy of those who interact with them.

Entities creating or using IoT should be open and transparent about the "who, what, where, when, why, and how" of data collection, transmission, processing, use, and disclosure.

Security + Safety

IoT projects and products should be designed, deployed, and maintained with security and safety in mind – to protect the public, ensure the integrity of services, and be resilient against physical tampering and cyberattacks.

Fairness + Equity

Projects and products should be designed and implemented with an eye toward public benefit and should be rigorously analyzed and corrected for bias and disparate impact.

Residents should be able to equitably participate in the IoT ecosystem.

Efficiency + Sustainability

IoT projects and products should be designed and deployed to minimize waste and streamline operations, and IoT infrastructure and resources should be shareable and reusable wherever practicable.

Environmental impact should be considered throughout the project or product lifecycle. Physical IoT devices, networks, and infrastructure should be used, maintained, and repurposed or disposed of in an efficient, responsible, and safe manner.

Openness + Public Engagement

Collected data should be made accessible whenever reasonable. Data ownership should be retained by device owners or users.

Entities using IoT should identify impacted populations and establish and use methods to engage with them for input before, during, and after deployment.

IoT Basics

In order to establish a baseline understanding of how IoT systems work, and the variety of technologies they can include, this section provides an outline of typical system architecture, a breakdown of common sensor types and the kinds of data IoT can produce, and a summary of the kinds of analytic systems that might be used to make use of IoT data.

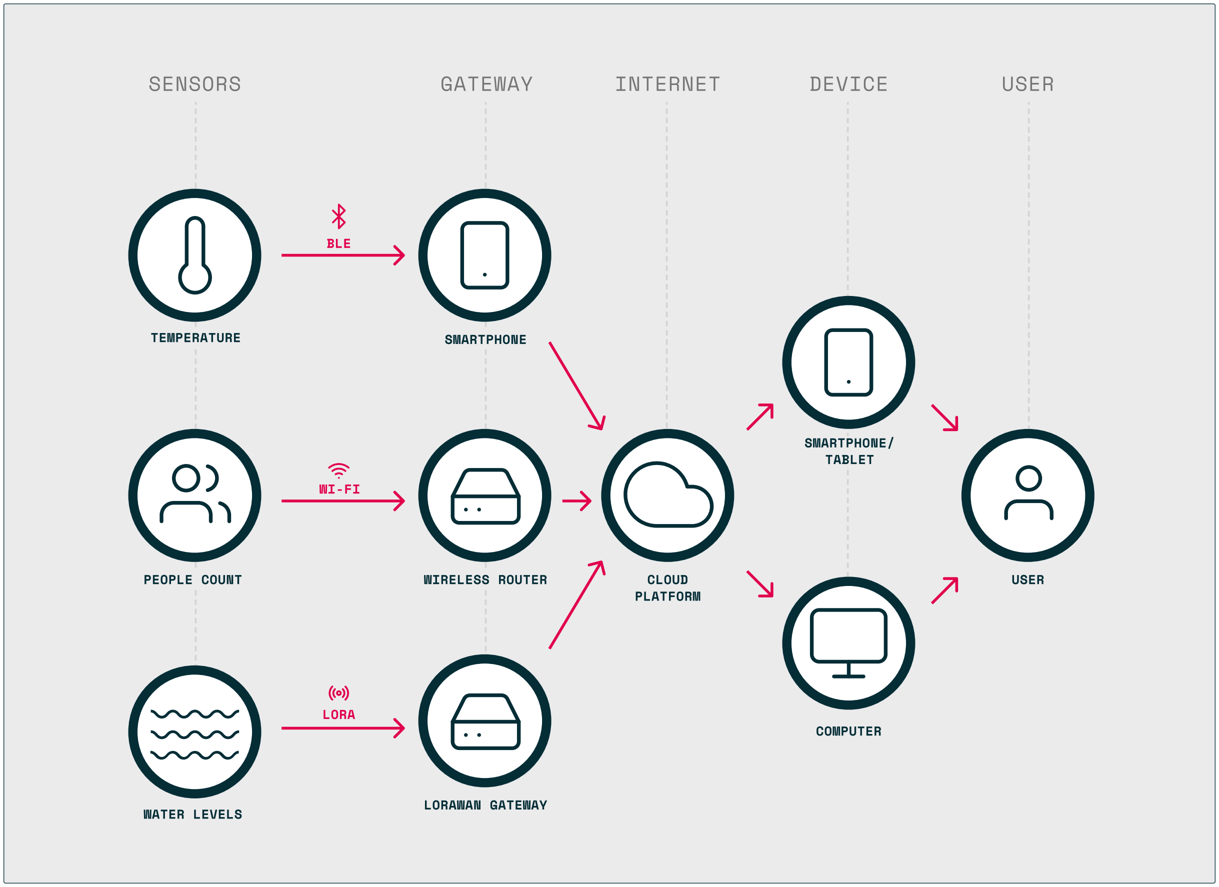
System Architecture

The following diagram illustrates a simplified version of a typical IoT system architecture. It starts with a sensor – such as a thermometer, vision-based sensor, or ultrasonic range finder (to determine water depths on a flooded street). These sensors collect data transmitted over a communications protocol – such as a Wi-Fi or cellular network – to a cloud platform on the Internet via a "gateway device," like a Wi-Fi router. The data are then sent to a web-based cloud platform or application where it is organized and analyzed. The cloud platform presents the data to a user via a computing device like a computer or smartphone.

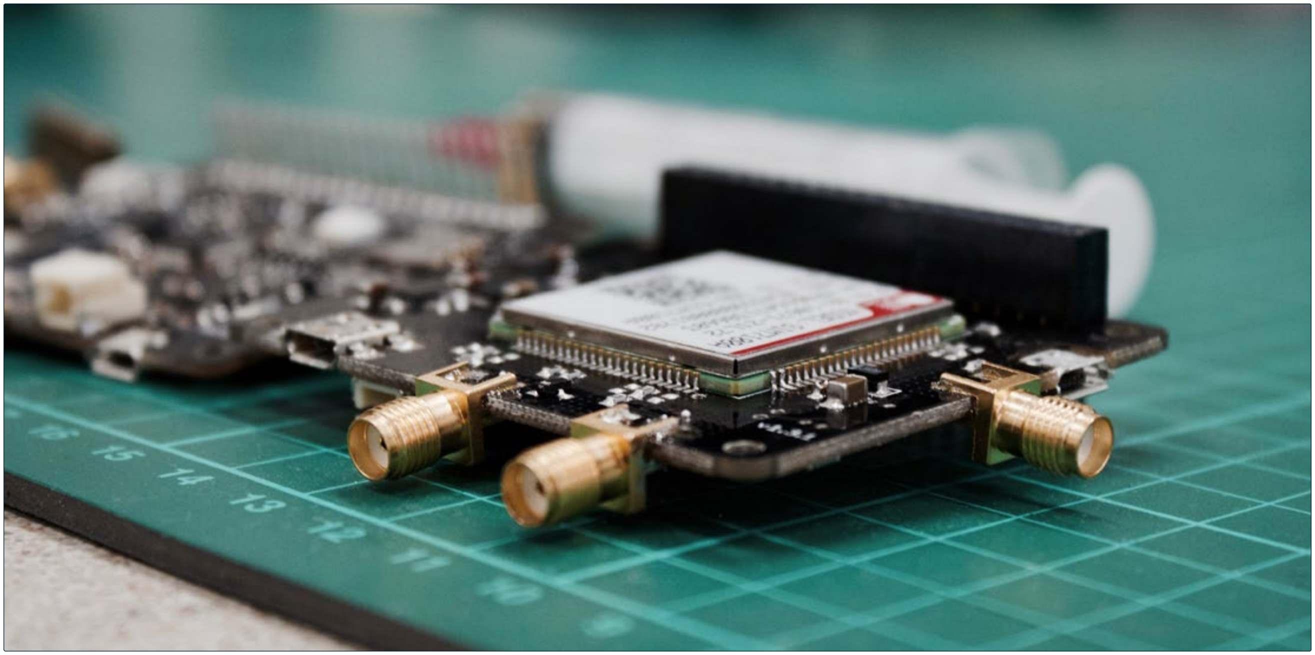
Sensors

At the core of most IoT projects are the sensors that collect data. While individual sensors vary widely, they can be sorted into the following categories.

- **Environmental**: These sensors are typically specialized and focused on collecting a specific type of data point, such as temperature, humidity, water or air quality, presence of gas and chemicals, or radiation, among others.
- **Vision**: Vision-based sensors can be adapted for multiple types of data, as such a sensor is essentially a camera that can be trained to "look" for an array of data types. Examples include object classification (person, vehicle, object, etc.), blob (basic object) detection, color detection, facial recognition, or infrared and heat detection, among others.
- **Acoustic**: Like vision-based sensors, acoustic sensors are adaptable to different scenarios where a microphone is listening for certain stimuli. An acoustic sensor might be listening to classify different types of similar sounds, like the differences between various engines' noise, or it could be listening for a particular type of sound like gunfire. Acoustic sensors are also used in voice assistant technology to listen for "wake" words that activate their language processing functions.
- **Electrical**: Electrical sensors take measurements of voltages and current in electrical systems. These would be implemented when trying to determine energy use or production like with "smart meters," as well as when diagnosing whether or not a machine is functioning properly.
- **Motion/Proximity/Presence**: These sensors typically measure the presence of or the distance to something or someone. Motion



[FIGURE 04 ▲] An example of basic IoT system architecture



[FIGURE 05 ▲] **A circuit board for developing an IoT sensor component.** *Photo: Louis Reed*

sensors often detect people, and proximity sensors can detect the presence and distance of objects – for example, water levels in a flood zone, or the presence of a vehicle in a parking space.

- **Location**: Location sensors, typically based on GPS technology, allow for objects or individuals to be located or tracked. These sensors can be used to track vehicles in a fleet (buses, trucks) or sensitive assets being shipped, such as medical supplies in a cold chain.
- **Radio**: Radio-based sensors encompass many different types of technologies and applications. For example, Bluetooth Low-Energy (BLE) beacons can send information to a smartphone about the user's location (wayfinding) and Radio-Frequency Identification (RFID) cards and tags can be used to gain access to buildings or pay tolls and monitor traffic flow (as with E-ZPass car tags).
- **Biometric/Biomedical**: These sensors detect physiological data that are either static and unchanging (biometric) or fluctuate over time (biomedical). Biometric sensors measure unique personal traits such as fingerprints, retinal scans, voice prints, or facial features. They are most commonly used for identification purposes, often as a security measure. Biomedical sensors often look at

Privacy Risk and IoT Data

Data collected by IoT devices carry varying levels of privacy risk that must be considered in making decisions about their collection, use, disclosure, and storage. Below is a framework for classifying three "tiers" of IoT data, based on privacy risk level. The framework is intended to be for informational purposes and does not represent a new classification structure used by New York City government.

The City of New York's Chief Privacy Officer established a set of *Citywide Privacy Protection Policies and Protocols* in 2019, which are publicly available.[072] These, and the City's *Cybersecurity Program Policies and Standards,* can be referenced for more details about privacy protection and information classification.[073]

TIER 1	TIER 2	TIER 3
Tier 1 data have no means of connecting to an individual's identity, location, or behaviors. They are typically environmental or aggregate/statistical in nature. There is little to no privacy risk expected in collecting these data with respect to individuals, except where aggregate metrics pertain to individuals in small groupings (e.g., <10) which, with other information, could lead to the identification of an individual. Typically, therefore, these data do not require the same scrutiny as the other tiers, although there may separately be policy, proprietary, or other legal considerations in disclosing these data. Unless one of the circumstances applies, Tier 1 data are likely to be classified as non-restricted information.	Tier 2 data are highly dependent on the context, detail, and the means by which the data are collected. Based on implementation, for example, Tier 2 data could either move up or down a tier to become restricted, sensitive, or non-restricted.	Tier 3 data will almost always be considered sensitive or restricted information and, if pertaining to individuals, are likely designated as confidential information by law. Personally identifiable information is sensitive or restricted by nature, or through its ability to be used in connection with other data to identify or locate a person. Collecting, using, disclosing, and storing this information should be limited, with appropriate prior legal review and safeguards in place to address any privacy or security concerns.
→ Ambient Temperature → Humidity → Air Quality → Energy Production (on-site) → Radiation → Water Quality → Water Levels (flooding) → Trash Volume/Servicing → Gas / Chemical → Greenhouse Gas Emissions	→ Traffic Counts * → Traffic Flow (Travel Time) * → Water Flow † → Energy Usage † → Sound Levels Δ → Pedestrian/ Cycling Counts ^ → Building Access/Usage ^ → Infrastructure Utilization ^ → Shared Mobility Utilization ^	→ Location Data (Vehicles, etc.) → License Plate / Car Tag Data → Biometrics → Health Data

Note: Data types in Tiers 1 and 3 will stay in those categories under normal circumstances. Data in Tier 2 may move, depending on various factors, such as how data collection is implemented. Each data type in Tier 2 is annotated, above, to indicate how data could become more or less sensitive.

* *Moves to Tier 3 (sensitive/restricted) if vehicle identifiers are captured*

† *Potentially sensitive/restricted if measured by individual unit*

Δ *Moves to Tier 3 (sensitive/restricted) if conversation content or biometrics are captured*

^ *Moves to Tier 3 (sensitive/restricted) if personally identifiable information (PII) is captured* physical vital signs like heart rate, blood oxygen levels, electrocardiograms, and are typically diagnostic in nature. Biometric sensors are commonly used in wearable technology like fitness trackers and smartwatches.

Data

The output of most IoT deployments is data. IoT data can be sorted into a few different categories, some of them overlapping, outlined below. This list is not exhaustive, but representative

- **Environmental**: Environmental data are collected from sensors located in a physical area of interest, either indoors or outdoors, and can represent natural or manmade inputs such as temperature, air quality, or sound levels.
- **Transportation/Mobility**: Transportation and mobility data can represent many aspects of how people get around like utilization of mobility infrastructure, number of pedestrians, or flow of vehicles on city streets. There is often a connection between mobility data and location data.
- **Location**: Location data are typically represented by coordinates created by a Global Positioning System (GPS) device. Real-time location can be provided to track the whereabouts of people, animals, vehicles, or other mobile objects.
- **Energy**: Energy data can represent the amount of energy a system produces, how much energy is being used, or the status of a heating/cooling system or lighting fixture.
- **Infrastructure**: Infrastructure data represent the status of infrastructure or machinery. This could be represented by connected trash receptacles, water pipes, building occupancy, or other such data points relating to built infrastructure.
- **Biometric / Health**: Biometric or health data represent information about a physical trait or characteristic of an individual and can be used as identifying information, for example: a fingerprint, face, or individual’s gait, etc. Health data represent short or long-term information about an individual’s or population’s overall health as it changes over time. This can be captured through a wearable device or through aggregate sampling, as in municipal wastewater.

Analytics

Once data are collected, IoT systems typically analyze those data to make them more useful and actionable. IoT analytics can be performed either on the device or in the cloud, and analysis may be presented as information in the form of dashboards, tables, alerts, or recommendations. The following categories describe how IoT data can be analyzed.

Descriptive analytics are the simplest and most straightforward form of IoT data analytics. They consist of capturing and describing the actual recorded data, such as temperature readings over time. Data can be presented in tables or through charts and graphs. Very basic data processing functions, such as calculating averages, are also considered "descriptive" in nature.

Predictive analytics, as the name implies, aim to predict outcomes based on historical data. Examples include predicting whether or not a pipe might burst based on measured leakage data or predicting when a machine component like a motor might fail based on a change in performance. In both instances, the prediction can spur preemptive maintenance to avoid an equipment or system failure.

Prescriptive analytics aim to take collected data and translate them into actionable recommendations for users. Beyond knowing what has happened from descriptive analytics or what could happen from predictive analytics, prescriptive analytics can recommend an action based on the data presented. This could manifest as a traffic management system recommending that an extra lane of highway be opened due to an increase in vehicle counts or balancing a bike share network by moving bikes from one station location to another.

There are additional terms and technologies that overlap with those mentioned above. Certain analytic tools veer into the realm of artificial intelligence ("AI") and machine learning, complex technologies involving terms with varying definitions depending upon context. The terms "algorithmic tools" and "automated decision systems" (ADS) have been defined by the City to guide appropriate use in City agency decision-making. These terms are distinct from but can overlap with IoT systems and the categories listed above, but a detailed discussion of them is out of scope for this document.[006]

IoT is varied and powerful technology, producing data with wide-ranging applications. The next section turns to an overview of how IoT is being used and considered today across society.

The Landscape

IoT Today

As IoT increasingly touches the lives of New Yorkers, it is important to understand the benefits these technologies can hold, as well as the risks they carry – whether encountered as individuals, organizations, or communities. This section presents an overview of how IoT is being used across a number of sectors, and the benefits and risks presented in each case, as well as how IoT is being treated from policy, legal, and educational perspectives.

Consumer Applications

IoT is appearing in consumers' lives today across a range of domains. There are wearable devices that can track our daily activity levels and biometric data, such as heart rate or sleep patterns, for health and wellness. There are products that automate everyday household tasks, from refrigerators that use cameras to track grocery inventory to vacuums that can be programmed and operated remotely. There are systems to maintain or monitor home security like smart door locks and interactive doorbells that can grant access or alert people of possible threats. Some help manage energy use by dynamically adjusting light or temperature based on our habits and use of space. There are even toys that respond and adapt during play, based on voice commands or visual inputs.

Consumer IoT products can offer significant value to users, in terms of health and wellness, energy and cost savings, and convenience and quality of life. At the same time, these products can present significant risks to privacy, safety, and data security. And the task of individually assessing the balance of potential benefits and harms can be daunting, particularly when manufacturers' privacy and data security standards are inconsistent, companies present their technology or terms in less-than-transparent ways, and data collection is invisible to the user.

[FIGURE 06 ▲] **A user checking a health tracking app on their smart watch.** *Photo: Solen Feyissa*

In recent years, there have been numerous cases in which user privacy and data security were compromised, or larger systems attacked, via consumer IoT products. Perhaps the best-known examples are the varied cases involving voice assistant technology. Integrated into smart speakers, wearable devices, and other IoT technologies, voice assistants have become increasingly popular among consumers for their ease-of-use and convenience – offering users the ability to speak commands or queries into a device and seamlessly get information or have the device perform tasks, such as playing music, taking notes, shopping, or placing phone calls. However, multiple cases have emerged in which users' voice recording data were erroneously shared with people on their contacts lists, or unknowingly sent to third-party contractors tasked with quality control and improving product algorithms.[007] Disturbingly, some of this data included casual conversation that would not normally be picked up without the use of a device "wake word."[008] A widely discussed example of consumer IoT being used to significantly disrupt the security of larger systems is the so-called "botnet attack," such as Mirai in 2016, where attackers

Trustable Technology Mark

For IoT device manufacturers, having clear policies around data privacy, transparency, security, and other digital rights is important to establish trust and accountability with consumers. While companies can share their stated policies and positions directly, third-party verification from a trusted source can also be an impactful way to garner confidence. For example, ThingsCon, a "global community and event platform for IoT practitioners" aimed at broadly supporting "a human-centric and responsible Internet of Things" is developing a "Trustable Technology Mark."[074] Such a license allows manufacturers to vet their products through a process managed by a trusted external party – in this case by ThingsCon. This model mimics other examples in industry, where third-party certifications are used, or sometimes required, for the sale of products (e.g., UL, FCC, or CE certification). Most current certifications that apply to IoT deal with safety or technical issues such as use of radio spectrum, where a certification related to trust and privacy is a more novel concept. The Trustable Technology Mark effort is in an early stage, but this type of third-party licensing and certification could be a powerful tool for supporting common standards and best practices in IoT.

Amazon Ring

In 2019-2020, Amazon's Ring subsidiary emerged as a highly public example of privacy and data security controversy in consumer IoT.[075] Offering a suite of home security products, including a home doorbell with an integrated motion sensor, camera, microphone, and speaker – which offers users the ability to remotely monitor and interact with visitors outside their door – the company has come under criticism for its internal policies and device security protocols, among other issues, in recent years.[076]

In 2019, the company's cameras were subject to several malicious hacking incidents. Taking advantage of weak user passwords and a lack of basic security features, such as multi-factor authentication, unauthorized users were able to "brute force" their way into user accounts and camera feeds. In some cases, these breaches included digital trespassers harassing device owners in their homes, via integrated device speakers.[077]

[FIGURE 07 ▲] A Ring camera positioned outside of a home.
Photo: Ring/Amazon

In early 2020, it was revealed that users' full names, email addresses, network and device information, and app usage – among other data from the Ring Video Doorbell's Android app – were being shared with third-party data analytics and marketing firms without transparent notification or request for consent from users.[078] This practice further allowed the third-party firms to recombine user data with data from other sources in order to track a broad range of individual digital activity.[079]

Ring's multifaceted relationship with law enforcement organizations has also raised concerns among consumers, as well as from civil liberties and civil rights groups.[080] Amazon has partnered with over 1,300 police departments across the United States to facilitate access to local networks of consumer Ring cameras for surveillance purposes.[081] Many civil liberties advocates see these relationships and practices as harmful to communities and democracy, supporting profiling of vulnerable groups, and skirting accountability processes with respect to data access.[082]

In response to these critiques, the company has taken steps to increase account security – limiting the number of incorrect sign-in attempts a user can make and enabling multi-factor authentication, for example.[083] Ring also updated its tracking policies in 2020 to allow users to opt out of some data sharing.[084]

[FIGURE 08 ▲] **Sensors monitoring industrial equipment.** *Photo: Crystal Kwok*

exploited consumer IoT device manufacturers' widespread use of default passwords to gain access to hundreds of thousands of IoT devices and used them to execute a series of distributed denial-of-serve attacks on major websites across the internet, rendering them inaccessible to their intended users. Consumers in the connected device market may also face a challenge when certain manufacturers close due to market failure or are acquired for their intellectual property. Because connected products generally rely on company-managed servers and software support infrastructure to keep products functional, IoT devices can stop working entirely when their corporate support is discontinued.

Industry Applications

Today, businesses of many types use IoT toward a wide variety of objectives and tasks – across manufacturing, real estate, mobility, agriculture, retail, service, and other sectors. Businesses are using sensors to track and manage inventory. They are integrating IoT-based monitoring to optimize operations – from maintaining equipment to re-designing processes and spaces. Businesses are using IoT to ensure efficient use of energy and monitor and mitigate security risks. They are using IoT to identify dangers to worker health and safety, and to manage and enhance employees' performance.

IoT integration can offer value to businesses of all sizes, in the form of operational optimizations, revenues and cost savings, or new or improved products or features. IoT utilization can support businesses' environmental and social responsibility goals by improving energy efficiency, reducing waste, and preventing harm to environments and communities.

In order to reap these benefits, businesses must make organizational and operational adjustments to integrate IoT technology and make use of new data. They must put new policies and standards in place to address interoperability needs, as well as internal and external concerns about data privacy, cybersecurity, trust, and fairness.

Importantly, the growth in industry's use of IoT also poses both benefits and risks for workers. On the one hand, the use of IoT can present new job or professional development opportunities, or make workplaces safer and more efficient. However, workers may have concerns about privacy and trust in their employers when subject to monitoring via IoT at work. They may face skills gaps in fields working to integrate the technology. And they may have concerns about wage or job security, where tasks or roles are automated.

Government Applications

The last decade has seen the rise of government use of IoT, particularly as municipalities work to develop as "smart cities." Utilizing environmental sensors, GPS, utility meters, counters, cameras, and other connected devices has given cities more expansive data at an unprecedented scale. Cities are using these data to measure environmental conditions, set goals, and manage interventions that result in improvements for residents. They are tracking their fleets to optimize operations and implement preventive maintenance. They are monitoring the use of energy to increase efficiency. They are analyzing the flow of people to better plan public space.

Governments can face a variety of challenges in integrating IoT. Coordinating between agencies, establishing effective governance, innovating with the latest technologies, sharing data and knowledge across departments, and safeguarding against cyberattacks are just a few of them. Among the biggest concerns that IoT technologies raise for governments, given their role as public servants, are those related to transparency, resident digital rights, and the responsible use of data. Governments also have a particular mandate to engage residents and incorporate their input into decision-making about how IoT is used.

In response to residents' concerns about privacy and transparency, cities are increasingly using "privacy by design" principles as they deploy IoT. The City of Melbourne, Australia, for example, has implemented a pedestrian-counting system that allows the municipality and its residents to monitor activity in different areas of the city to "better inform decision-making and plan for the future."[009] Recognizing the risks to residents' privacy, and to

Fairness and Equity in IoT

Fairness and equity are of critical concern to fostering a healthy IoT ecosystem, and the risks of bias or disparate impact in IoT are multifaceted. Sensor technologies, for example, can present bias risk – particularly when they interact with human physical traits such as skin tone, height, body composition, or use of assistive devices, among others. Some fitness tracking devices, for example, show decreased performance when tracking heart rates in people with darker skin or who have higher body fat, with impacts that can range from relatively minor inconvenience to adverse health outcomes due to inaccurate readings being sent to medical providers.[085] Equity and fairness risks can also come into play in broader IoT project design. Location selection of sensors, for example, can have significant impact on whether data collection is representative of all populations or communities. Additionally, decision-making based solely on IoT data can miss important contextual factors, which could lead to inequitable solutions. For example, if a city were to assess mobility needs based solely on IoT-based bicycle counts, they could misinterpret a lower number of bikes present in a lower income neighborhood as a lack of demand for bikes, rather than a lack of access to them. If those data were then used to select where to place cycling infrastructure, inequities could result by neglecting to add infrastructure in areas that, in fact, need that support most. Use and placement of ”surveillance“ technologies can additionally pose inequitable privacy risk, or inequitable harm in terms of real or perceived monitoring of everyday activity. There is evidence that communities of color and low-income communities, in particular, are disproportionately subject to surveillance for various purposes.[086] It is important to keep this in mind when selecting technologies as well as communicating the purpose and methodology of an IoT project. Data analytics, algorithms, and decision systems can also present varied and significant risks of bias, but a deeper look into those systems is out of scope for this document.

Participation in the IoT ecosystem, and access to the opportunities it presents is another key area of concern for fairness and equity. On the one hand, IoT products or connected public assets can be inequitably available, due to means, knowledge, or distribution across communities. Bike- or scooter-share distribution has been a particular area of focus in cities in this regard – an issue community groups such as the Bedford Stuyvesant Restoration in New York partnered with the City and Citi Bike to address, for example.[087] On the other hand, equitable empowerment in interacting with IoT across society is another key concern. This applies to residents’ ability to use consumer products, understand and provide input into systems in place across society, use and critique data to varied ends, and obtain work and advance careers.

their trust in the local government, Melbourne collects no personal information in the project – recording only movement, not images. Additionally, the project's data are shared publicly via an interactive data visualization website, so that residents can freely use it as a resource, alongside civil servants.[010]

Cities – such as Copenhagen, Helsinki, and Las Vegas – are also increasingly designating discrete "living lab," "testbed," or "innovation zone" areas to increase their capacity to experiment with emerging technologies and applications - including those related to IoT.[011] These designations allow cities to more easily partner with industry to test new technologies through a standardization of practices. Standard partnership agreements establish working relationships and legal terms between City entities and industry stakeholders. Establishing wireless networks, power access, mounting points, and other accessible infrastructure in the testbed reduces starting costs and work required before each test. Establishing community buy-in for the larger initiative can also reduce conflicts that might arise from ad hoc projects.

Community Organizations

Community organizations are engaging IoT in a variety of ways today. Business Improvement Districts (BIDs), non-profits, and other community groups are deploying IoT, or using external IoT data to support their operations and justify investment. They are using it to improve services and provide rapid response to hyperlocal concerns. They are engaging residents with IoT through workshops or training programs to deepen civic engagement and build new skills.

Community groups confront many of the same challenges that businesses and government entities do in working to integrate IoT. They are faced with organizational capacity and governance challenges, privacy and security concerns, and the need to be transparent with patrons and community members about the technology they use. These groups can also have difficulty accessing or using data from outside entities or finding avenues for productive partnership across sectors. Finally, community organizations that offer public engagement and education services can lack capacity to keep pace with advances in the technology and evolving IoT workforce needs.

Policy Approaches and Legislative Actions

As the Internet of Things has become an increasingly prominent feature of contemporary life, governments have had to explore their roles in regulating IoT use in the public and private sectors. Policy interventions have spanned all levels of government and range in form from guidance to legal mandates. Policy and legislative actions have, to date, focused significantly on privacy and security, as well as transparency and public accountability.

With few exceptions, federal legislative approaches in the United States have been piecemeal, leaving states and municipalities to enact their own laws and protections. Certain measures have focused on ensuring appropriate cybersecurity protocols are in place when governments deploy IoT devices, to guard against threats to public infrastructure and systems. The "Internet of Things Cybersecurity Improvement Act," signed into law in late 2020, requires the development of standards and guidelines for the use and management of IoT devices "owned or controlled" by the federal government, including "minimum information security requirements for managing cybersecurity risks."[012] California's IoT Security Law, passed in 2018, was the first U.S. state law to establish requirements related to IoT security. It requires manufacturers of IoT devices sold or offered for sale in the state, to include "reasonable security feature or features ...designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure..."[013]

Other measures have focused on IoT privacy and transparency. The City of Seattle has taken a holistic approach to addressing privacy, security, engagement, and transparency in government use of IoT and related technologies. In 2017, it enacted an ordinance to "provide greater transparency to City Council and the public when the City acquires technology that meets the City's definition of surveillance."[014] The ordinance requires City departments to prepare public "Surveillance Impact Reports" containing a range of details about an IoT deployment. These include a description of the technology and project goals, data that are being collected and how it will be used and stored, community engagement conducted, and notifications in place to alert the public to the presence of a "surveillance" device and where they can find more information about it, among other items. Notably, the ordinance also specifies that these reports must contain an explanation of how the relevant department has taken into account the technology's "potential impact...on civil rights and liberties and disparate impacts on communities of color and other marginalized communities."[015]

Still other measures have sought to simply establish commitments to learn more about the variety of policy and legal issues raised by IoT technology. In 2020, the U.S. Senate passed the "Developing Innovation and Growing the Internet of Things (DIGIT) Act." The bill would direct the U.S. Secretary of Commerce to create a working group of federal stakeholders to broadly study the ramifications of the growth of the Internet of Things.

Several states have passed broader consumer privacy legislation that applies to IoT. California's Consumer Privacy Act, enacted in 2020, affords residents of the state an array of rights with regard to information of any kind that businesses collect about them, including through IoT technologies. The statute provides residents the "right to know" the personal information businesses collect and how it is used and shared, the "right to delete" such

Chicago's Array of Things

The City of Chicago and its partners have particularly emphasized community engagement and public awareness in designing and deploying the Array of Things ("AoT") initiative — a "collaborative effort among scientists, universities, federal and local government, industry partners, and communities to collect real-time data on urban environment, infrastructure, and activity for research and public use."[088]

In advance of project deployment, the City and its collaborators worked with a set of community and civic organizations with expertise in community engagement, in order to build public awareness about the project, assess community needs, and gather input on draft governance and privacy policies. The City and its partners offered multiple channels for public input, holding community meetings, as well as offering several online channels for suggestions and policy input. They established a program to recruit community members to attend and help document community events, and documentation was produced and published in multiple formats in order to reach diverse communities.

Feedback gathered through these channels was used to update and finalize project governance and privacy policies, which were then published on a public website.[089] Public input also informed the design and deployment of the project itself, and channels were established to gather public input on an ongoing basis.

Project partners additionally worked with local public high school to design an eight-week course to support resident understanding of the project from an early age.

Finally, data from the project are openly available for public use, via the City of Chicago Data Portal, and other platforms.[090]

[FIGURE 09 ▲] An Array of Things sensor node gets inspected before being mounted in Chicago.
Photo: Rob Mitchum, University of Chicago

information collected, the "right to opt-out" of this information being sold, and the "right to non-discrimination" for exercising these rights.[016]

Illinois' 2008 Biometric Information Privacy Act regulates how private entities doing business in the state collect, store, and share biometric data, information that could be collected by IoT devices.[017] The law requires companies to obtain informed consent for collection of data, as well as any disclosure of them to other entities. It prohibits companies from profiting from collected data. And it sets security requirements for the storage and transmission of these data. Texas passed a similar Capture or Use of Biometric Identifiers law in 2009, and Washington followed suit in 2017 with its H.B. 1493.[018]

Some local governments have mandated Privacy Impact Assessments (PIA) for internal initiatives, broadly. The county of Derbyshire in the United Kingdom, for example, put PIA procedures in place in 2017 in order to ensure that any project undertaken by the county maintains compliance with applicable data protection obligations, and can minimize risks to resident privacy, while upholding key project goals.[019] These practical procedural interventions can be impactful ways to ensure consistent, proactive analysis and mitigation of privacy risks, while upholding project implementation timelines and impact. They can be a useful guidance and governance tool for collection and management of personally identifiable or other sensitive information, when required.

The most far-reaching international law impacting privacy and data security is the European Union's (EU) 2018 General Data Protection Regulation (GDPR).[020] Applicable to organizations across the world, the law is intended to protect EU residents' privacy and data security and allow them to control how their personal data are used – across a broad range of technologies and products, including IoT. The law requires measures to secure user consent, promotes "privacy by design" principles, and empowers users to decide how their data are used, among other components.

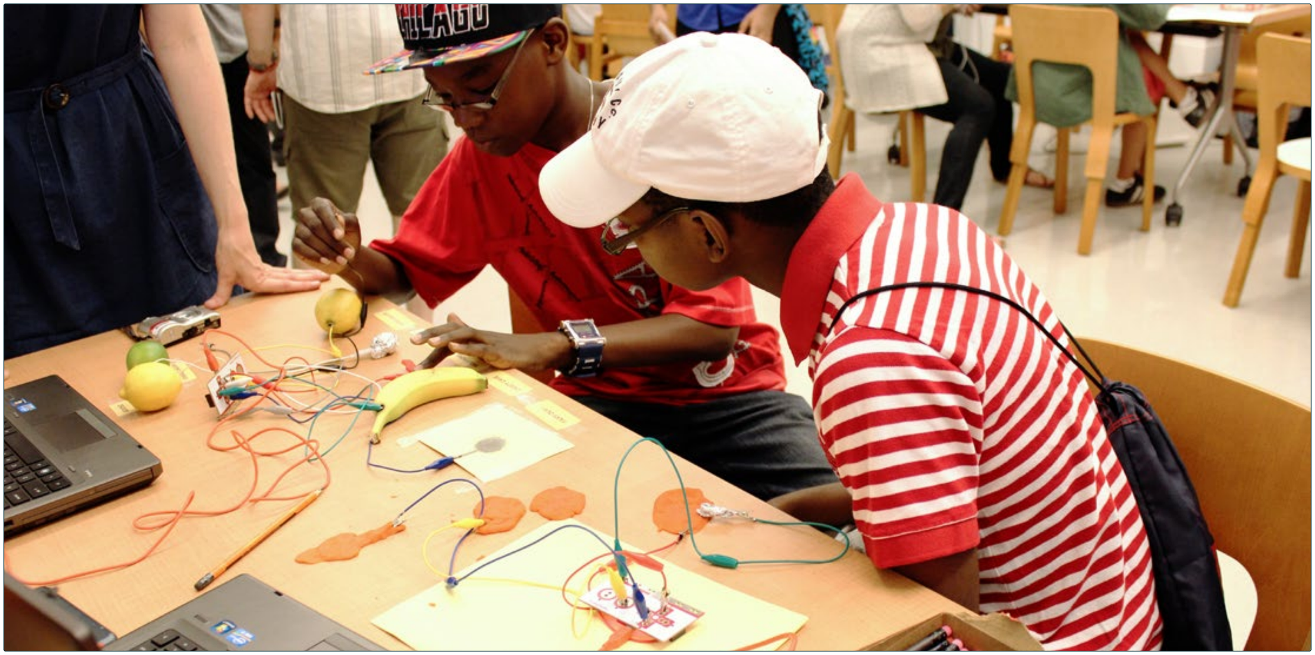
Beyond these policy and legislative actions, governments have also sought to influence IoT technology and privacy concerns via published guidance. In 2020, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) put forward a Privacy Framework – a "voluntary tool" intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy."[021] The Framework offers organizations a starting point for identifying desired privacy outcomes and outlines steps toward achieving them, such as developing data safeguards, managing data "with sufficient granularity to meet privacy objectives," maintaining transparency as to how the organization manages data, and developing appropriate responses to any privacy breaches.[022]

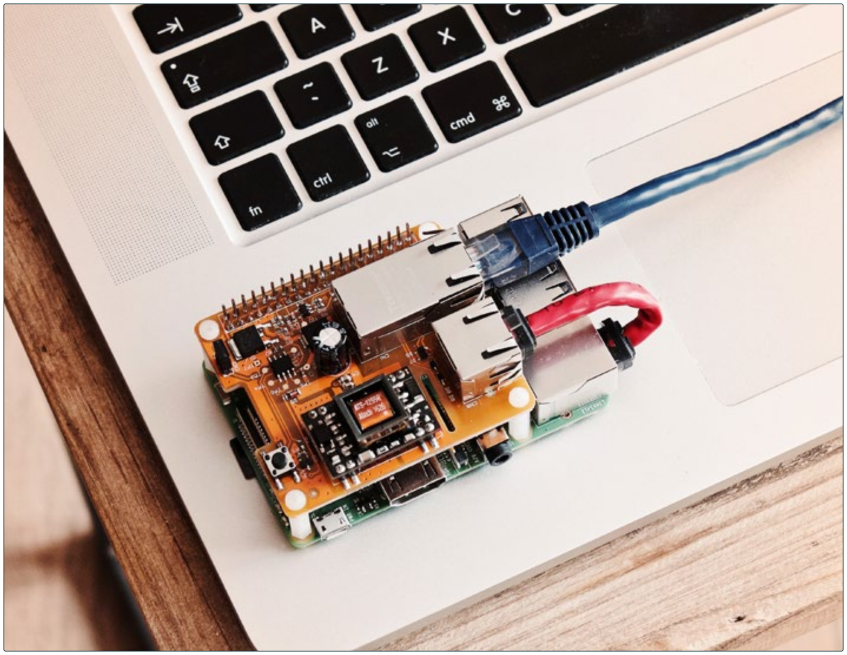
Education and Training Approaches

IoT-related subjects are making their way into a range of education settings, from school coursework, to extracurricular activities, to age-spanning digital literacy programs and public awareness campaigns. Subjects span direct training on the use of consumer IoT, integration of IoT technology in broader applied science programs and projects, as well as programs that teach skills and subjects foundational to engaging with IoT, such as physical computing, data literacy, and privacy and data security. Public awareness campaigns can touch on some of these subjects but typically also aim to increase transparency about where and how IoT is being used in public space.

STEAM Expeditions' R.E.M. Team in Jersey City, NJ

Extracurricular programs can offer students opportunities to engage in long-term, applied IoT projects. At P.S. 28, a K-8 public school in Jersey City, New Jersey, student members of an afterschool STEAM program identified a need to alert community members of possible environmental hazards, following an explosion and fire at a chlorine plant in Kearny, New Jersey.[091] An all-female Remote Environmental Monitoring ("R.E.M.") team – one of several teams enrolled in the larger STEAM Expeditions program – deployed a variety of IoT devices to monitor air and water quality in their community, toward increasing public awareness of hazardous conditions. The team identified and purchased sensors, conducted outreach to secure approval to deploy them in public spaces, designed and constructed housing for their equipment, set up gateway devices, and connected them to The Things Network, an open, community-run LoRaWAN network.[092] They then developed a website, social media accounts, and print materials to communicate with the public about the project.[093] After deploying their initial project, the team expanded to new applications and school partnerships. Sponsor teachers work to foster partnerships with academic and industry stakeholders to provide feedback and guidance and to offer students opportunity to present new ideas and perspectives back to the field. In April of 2020, the R.E.M. team project won the middle school Grand Prize in the 2020 Lexus Eco Challenge competition.[094] In late 2020, the program began working with a local university's business school to help students develop business plans for their projects to boost their sustainability across cohorts, and incorporate the possibility for students to commercialize their projects.





[FIGURE 10 ▲] Teens learning about electronics at Brooklyn Public Library.
Photo: Brooklyn Public Library, CC BY-NC-SA 2.0

[FIGURE 11 ▶] A circuit board for developing IoT hardware applications.
Photo: Louis Reed

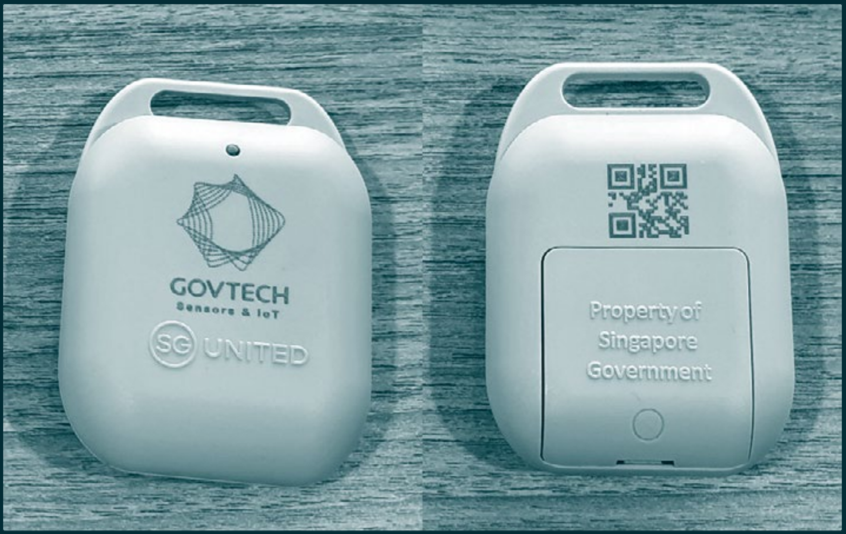
IoT and COVID-19

COVID-19 has presented a multifaceted crisis across the globe, and governments, industries, and individuals have been faced with finding new ways to respond and adapt. IoT has played a role in these shifts in a variety of ways.

Government Use: Many governments have pursued "digital exposure notification" applications to support – or, in some cases, replace – COVID-19 contact tracing efforts. This approach typically utilizes a BLE radio device, embedded in smartphones or in standalone key fob-like devices, to track proximity of individuals and identify potential exposure to COVID-19. Australia's government, for example, has developed COVIDsafe, an app available to download for Bluetooth-assisted contact tracing; the collected data are encrypted, kept for 21 days, and then deleted. Singapore has also developed a contact tracing app, TraceTogether, along with its SafeEntry program which involves checking-in to certain locations like restaurants and shopping centers to aid in contact tracing.[095] The app is voluntary for residents but required for all visitors. Singapore has also developed standalone "tokens" which can be used by residents who do not have smartphones, ensuring that all who want access have the ability to use this technology.[096] Most nations have taken an "opt-in" approach to implementing these apps, with a few exceptions, such as South Korea, which mandated use of its own app in order to enforce quarantine requirements for travelers arriving into the country as well as wristbands issued to those who have broken quarantine restrictions.[097]

New York State rolled out the COVID Alert NY contact tracing app in October of 2020, which aims to reduce the spread of COVID-19 within the state through digital exposure notification.[098] Use by New Yorkers is voluntary. The open-source app is based on Bluetooth technology and a notification system developed by Apple and Google in conjunction with MIT.[099] It works by privately and securely exchanging digital tokens if a user comes within six feet of another user for ten minutes or more. When an app user tests positive for COVID-19, they can anonymously share their contact list with the Department of Health for notification of possible exposure. No identifying information is shared. In the first month of use, the app had been downloaded half a million times.[100]

IoT is also being used by public entities around the world to manage density in public spaces, and screen



[FIGURE 12 ▲] Singapore's BLE-based exposure tracking "tokens."
Photo: Roland Turner, CC BY-SA 3.0

for symptoms of COVID-19. For example, New York City's Metropolitan Transportation Authority (MTA) has recently added a feature to their website and the MYmta app that reports the density of New York City buses by counting passengers using "infrared sensors and 3D image pattern technology."[101] MTA Long Island Rail Road has added a feature to its TrainTime app that calculates how crowded each train car is in real time using the weight of each train car or a system of infrared sensors that count passengers as they board and leave the train.[102] MTA Metro-North Railroad subsequently incorporated a similar real-time capacity tracking feature in its app and on station signage to enhance social distancing.[103] Finally, in Taiwan, the Taipei Metro system began using infrared thermography to screen passengers for fever and prohibiting anyone measuring a temperature above 38 degrees Celsius from entering.[104]

Wastewater testing has also emerged as a method for COVID tracking using IoT. For example, Israel-based company, Kando has been working with municipalities across the world to deploy sensor systems in public sewers to identify the presence of coronavirus in wastewater. Cities are using this technology to find potential COVID-19 hotspots before they are visible through sick residents.[105]

Governments have also turned to working with private companies to integrate data from consumer devices. Kinsa Health, which makes an internet-connected smart thermometer, has begun publicly sharing aggregate temperature data from ill residents during the COVID-19 outbreak that shows strong correlation to coronavirus cases. Governments and non-profits in California, Colorado, Connecticut, Idaho, Oregon, New Orleans, Albany, New York City, and Philadelphia are deploying Kinsa's connected thermometer devices or are integrating its health data.

Corporate Use: Businesses are also using IoT in new ways during the pandemic. In opening the 2020-2021 season, the National Basketball Association (NBA) offered players "smart rings" that use sensors on the wearer's finger to detect possible COVID-19 symptoms, ranging from fever to heightened respiratory rates.[106] Las Vegas Sands, which owns the Venetian and Palazzo resorts has also deployed smart rings to 1,000 staff members to detect the early onset of COVID-19 symptoms.[107]

While wearables such as smart rings offer near 24/7 monitoring of symptoms, many companies are deploying IoT devices at their facilities in order to screen employees for fever symptoms. Although efficacy is mixed, infrared thermography or infrared non-contact thermometers are often used by staff to screen employees, but there is a growing subset of products that are standalone IoT devices, without direct human involvement. These devices can connect to building systems to grant or deny access through electronic gates and doorways or send alerts to onsite staff to investigate further[108].

Healthcare: With an influx of patients due to COVID, hospitals have worked to limit interpersonal contact. IoT technology has been integrated to this end in a variety of ways. In Wuhan, China's Hongshan Sports Center, for example, a hospital used almost no doctors or nurses. Instead, it relied on an enormous network of connected thermometers, wearable symptom-monitoring bracelets for patients and staff, autonomous food and medicine delivery carts, and robots designed for sanitizing and entertainment.[109]

Privacy and security are particularly important in applications that use health-related data. In order to build trust in technology and institutions, it is critical that governments, corporations, and healthcare institutions alike maintain high standards in how they handle sensitive data.

IoT in NYC

In New York City, IoT is being used and considered in many of the varied ways described above. This section highlights some of its key treatments across the city's public, private and non-profit sectors.

Municipal Use

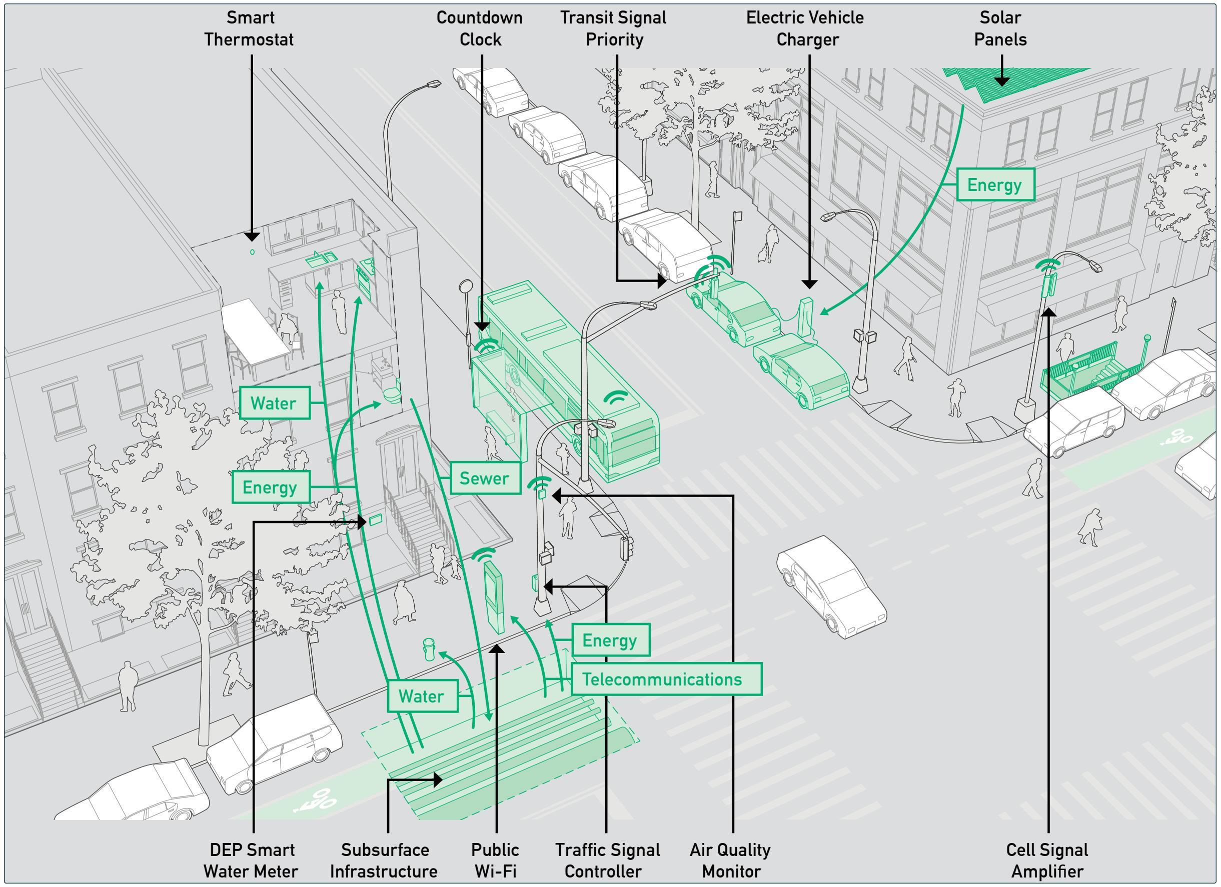
In New York City government, there has been a steady increase in the use of IoT technology over the last ten years, across a wide range of agencies and projects. The City has used IoT to monitor air quality, temperature, and other weather data, to analyze traffic patterns and count cyclists, to track City-owned vehicles, assess energy usage, and maintain water mains, among other examples.[023]

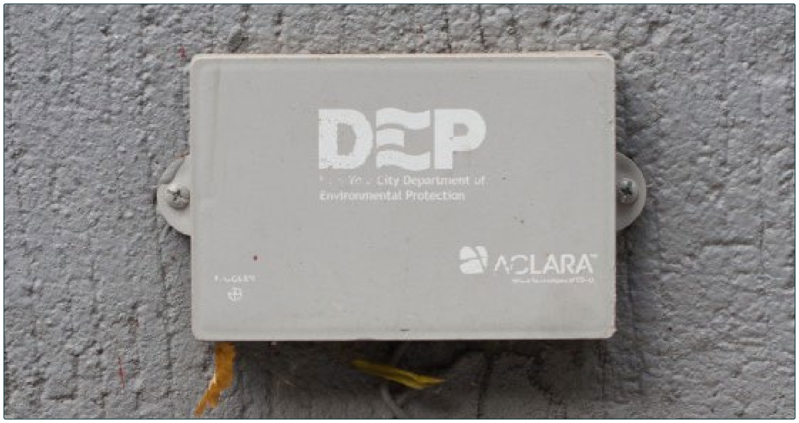
Among the City's largest-scale IoT projects is the Department of Environmental Protection's (DEP) integration of wirelessly connected water meters for buildings.[024] These meters allow DEP to monitor water usage in over 800,000 buildings across the city, eliminating the need to send physical inspectors to read meters. The system also allows the City to alert residents when they might have a leak, based on tracked increases in use, or whether a building is inhabited when it isn't supposed to be, among other benefits.

Another large-scale example is the Department of Citywide Administrative Services (DCAS)'s implementation of the nation's largest tracking program for public vehicles.[025] Launched in 2018, the Fleet Office of Real-Time Tracking (FORT), uses a ”telematic“ system (comprised of telecommunication, vehicle, and sensor technologies), to track 23,000 fleet vehicles across fifty City agencies and forty public school bus companies, logging data on vehicle locations, utilization, and maintenance needs, as well as crashes, speeding infractions, seatbelt use, and idling. Data from the project are being used to improve City services, support safety, maintain fuel and resource efficiency, and prepare for emergencies – all with enormous implications for cost, sustainability, service quality, and public safety.

Acknowledging the sensitivity of vehicle location data, DCAS has implemented a set of internal security policies and procedures for access to and management of the program data. DCAS has also anonymized the data when used in conjunction with external partners, such as universities, for analytical purposes.

The City is also using IoT to automate enforcement of traffic laws and boost public safety. Part of the City's broader Vision Zero initiative to improve the safety of city streets, the Department of Transportation's (NYC DOT) Speed Camera program uses connected cameras to remotely enforce speed limits in City school zones.[026] First launched in 2014, the program was expanded in 2019, when a State law was passed enlarging areas and hours allowable for speed camera use.[027] It now covers all 750 school zones allowable under the law. The deployed cameras identify vehicles



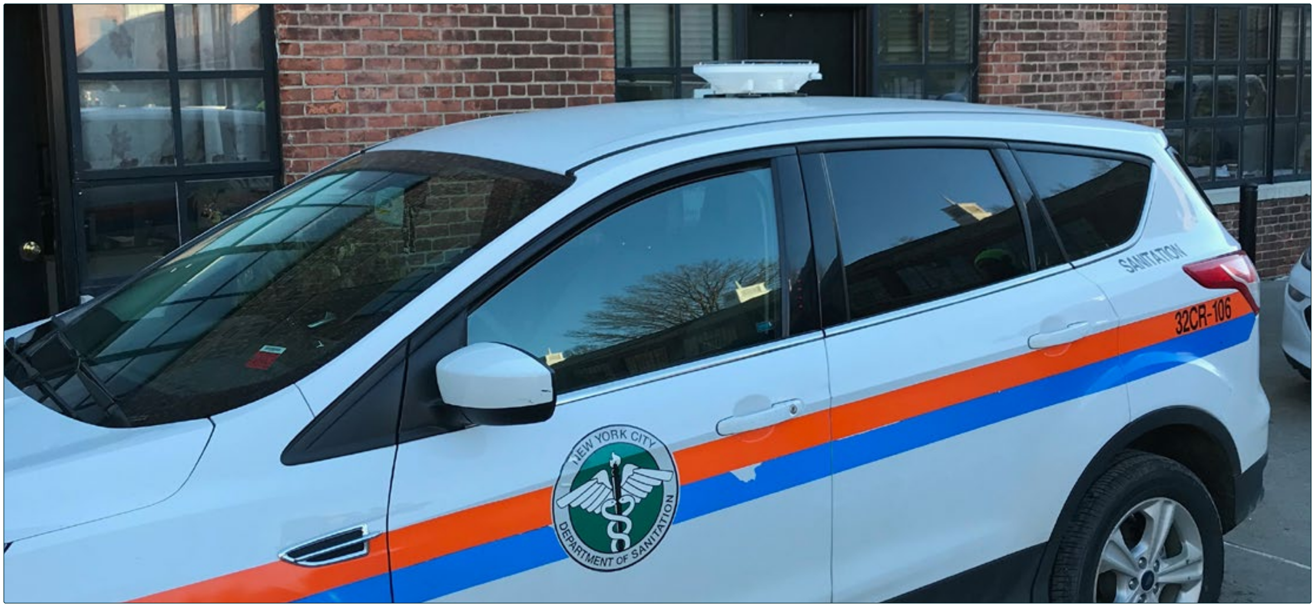


[FIGURE 13 ▲] This diagram of a "connected city" first appeared in *OneNYC 2050* where the City's IoT Strategy was committed to being developed.

[FIGURE 14 ▶] A Department of Environmental Protection building water meter. *Photo: Mayo Nissen* travelling ten miles per hour or more above the posted speed limit, capture an image of vehicle license plates, and issue a $50 notice of liability to the registered vehicle owner. Data from the initial camera rollout showed that speeding in zones with a camera declined by more than sixty percent, and that the majority of violators did not receive a second ticket. The DOT's Red Light and Bus Lane camera programs are two other example in this vein.[028]

It is worth noting that many cities are looking to automated enforcement as a means of reducing local law enforcement involvement in low-level traffic violations. Some civil and constitutional rights advocates believe this model can help create more equitable cities by removing the discretionary elements of human-led traffic enforcement.[029]

NYC DOT began a 75-month research and pilot program in 2015 that was part of a U.S. Department of Transportation-funded initiative to study Connected Vehicle technology.[030] The NYC Connected Vehicle Project (CVP), is "primarily focused on safety applications – which rely on vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and infrastructure-to-pedestrian (IVP) communications."[031] Aside from using this technology to prevent collisions between vehicles, there are also applications that aid blind and low-vision pedestrians with street crossings, and those that monitor compliance with speed regulations in work zones or height restrictions for oversized



[FIGURE 15 ▲] An MIT CityScanner sensor node on top of a New York City Department of Sanitation vehicle.

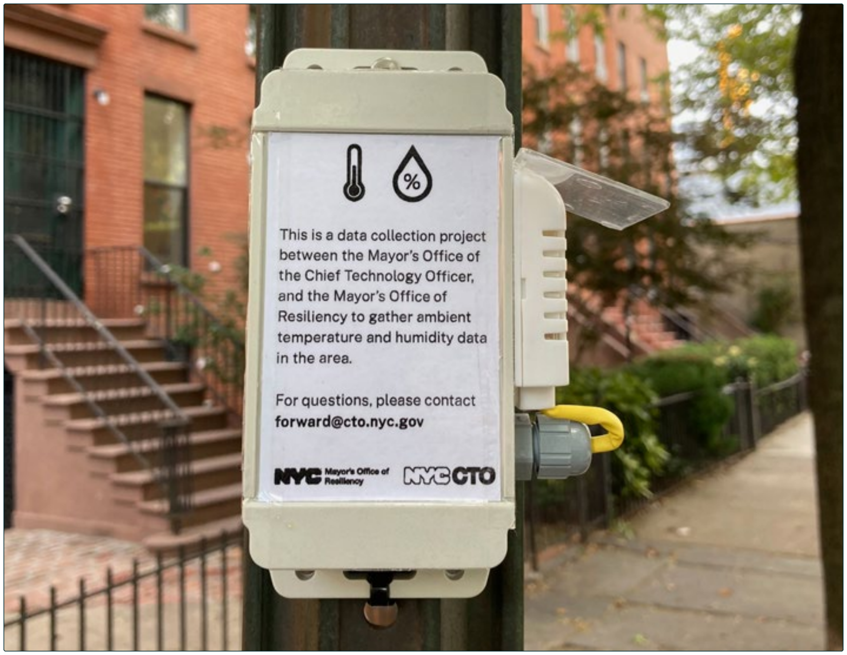
vehicles, among others. This project shows how New York City's collaborative approach to cutting-edge research and development can have impact throughout the country, making cities safer for people through the use of connected technology.

In 2020, NYC DOT completed the conversion of its traffic signals, camera, and travel sensor network from the end-of-life NYCWiN network, which has been discontinued citywide, to a new Traffic Safety Network (TSN), creating the City's largest IoT communications network. TSN connects over 13,000 intersections and devices to DOT's Traffic Management Center – providing situational awareness of City road use and facilitating advanced applications like adaptive traffic control and Transit Signal Prioritization to improve bus travel speeds.

Additionally, NYC DOT is using IoT to provide customer-facing benefits, and ease operations, management, and enforcement of metered parking across the city. In 2016, the agency launched ParkNYC, a mobile platform for parking payments.[032] And in 2021, NYC DOT plans to begin installing Pay-By-Plate meters, which will facilitate the introduction of new curb management techniques, enhanced analytical capabilities, and opportunities for more effective enforcement.

The City is also testing new approaches through a range of experimental programs. In January of 2020, the NYC Department of Health and Mental Hygiene partnered with NYC CTO and DCAS to create a pilot program in collaboration with the Senseable City Lab at the Massachusetts Institute of Technology.[033] The Lab's CityScanner project is a low-cost alternative to traditional methods of collecting environmental data. The solar-powered sensor nodes attach to the roof of City vehicles and collect more hyper-local data than traditional fixed-position sensors. Sensors capture environmental data, such as air quality, temperature, humidity, and road conditions, and they record that data to an online database. The first four-week pilot of the initiative in New York City took place in the South Bronx, a neighborhood known to have a history of below-average air quality. The data are being used to identify potential air pollution "hotspots," or areas that have particularly elevated emission levels, in an effort to identify and address their sources.

In another partnership with academia, the Mayor's Office of Resiliency and NYC CTO partnered in April of 2020 with the City University of New York and New York University to co-develop a first-of-its-kind, real-time flood monitoring system for parts of Brooklyn and Queens. Funded by a grant from the Empire State Development Corporation, as well as university contributions, the project is deploying internet-connected sensors in flood-prone neighborhoods to measure the number of flooding incidents, as well as their depths. Sensors will rely on the LoRaWAN-based Things Network for communication and will require new gateways to be installed. As part of the pilot, the City will test the efficacy of the network and identify whether or not it can be a


This is a data collection project between the Mayor's Office of the Chief Technology Officer, and the Mayor's Office of Resiliency to gather ambient temperature and humidity data in the area.
For questions, please contact forward@cto.nyc.gov
NYC Mayor's Office of Resiliency
NYC CTO

[FIGURE 16 ▲] A temperature sensor installed in Brooklyn for a rapid IoT pilot with MOR.

useful tool for future sensor deployments. The project will produce a software tool that will allow residents, NYC infrastructure and emergency management agencies, and researchers to directly monitor the incoming data and receive alerts about weather events. This data will help inform flood mitigation efforts and calibrate future flooding models. Further, NYC CTO will pilot new IoT transparency signage as part of the deployment, aimed at supporting public awareness about the project, its goals, and the data being collected. NYC CTO will gather feedback from City agencies, collaborators, and residents on the efficacy of this signage, toward developing it for potential broader use in City IoT projects.

In the summer of 2020, NYC CTO launched a "Rapid IoT" proof-of-concept, which aims to approach IoT from the perspective of short-term, low-cost device deployments to gather data for immediate insights as well as more in-depth study. Each Rapid IoT deployment could be seen as a proof-of-concept for a larger informational or operational IoT project. In the summer of 2020, NYC CTO tested the concept by gathering temperature and humidity data for two weeks on behalf of the Mayor's Office of Resiliency. In a period of just four weeks, the NYC CTO Smart Cities & IoT Lab designed and fabricated the sensors and established the data communications and dashboard to monitor and analyze the incoming data.

In 2021, the NYC DOT and NYC CTO, will pilot computer vision technology to provide automated counts of pedestrians, cyclists, and vehicles as they move through parts of the city, with funding from the Empire State Development Corporation. This type of work is currently conducted by hand and is labor- and cost-intensive. Having more rigorous data sets about how mobility habits and patterns are changing will enable DOT to assess street design and road infrastructure to better accommodate the evolution of transportation within the city. This year-long pilot is being approached with "privacy by design" principles, and the selected sensors will not be transmitting any image or video data from the device, except during a brief calibration period. This approach allows the City to take advantage of the advanced classification and counting capabilities that come from vision, but without the privacy concerns associated with video transmission and recording. During the course of the pilot, the City will engage with residents to gather input on the technology and will test a version of a privacy and equity impact assessment that could serve as a model for future IoT projects.

In addition to deploying IoT in new ways, the City is also establishing capacity to to perform in-depth analysis of the cybersecurity of IoT devices and systems and the networks on which they operate. In 2017, Mayor Bill de Blasio established NYC Cyber Command (NYC3) to lead New York City's cyber defense and response, working across agencies and offices to "prevent, detect, respond, and recover from cyber threats."[034] In order to examine cybersecurity in City IoT deployments, NYC3 has built processes to review and test devices and networks that City agencies are procuring. Protecting the security of City systems is of the utmost importance, and NYC3 is working to ensure that IoT deployments in New York City are safe and secure.

NYC CTO has also worked to prototype and pilot a set of coordination and governance tools for the City in recent years. In 2018, NYC CTO launched the City's first-ever IoT device inventory initiative. While the project was preliminary, producing only a partial picture of City efforts, it represented an important first step toward developing a full, citywide catalogue. In 2018, NYC CTO also launched a monthly working group for IoT coordination amongst agencies. This group has particularly focused on expanding existing City technology review processes to include interoperability, and varied digital rights concerns, such as security and privacy, among other topics. Finally, in 2019, NYC CTO created a proof-of-concept near-real-time data dashboard for City IoT devices. The software demonstrates how multiple, unrelated City data streams can be ingested, analyzed, compared, and shared between agencies and to the public. The tool represents a starting point toward making data more accessible and actionable across the City.

Industry Use

Businesses in New York City are developing and deploying IoT solutions to meet 21st century needs and improve the way they work. From real estate to mobility, energy to agriculture, IoT is changing the way companies operate in New York City. City businesses engage with IoT across sectors, with a range of examples too numerous to describe in detail here. Below are just a few examples that illustrate the scope and diversity of ways industry contributes to and participates in New York's IoT ecosystem.

IoT has played a significant role in the city's mobility sector over the last decade, and most New Yorkers would be hard-pressed not to have noticed the changing streetscape and available options for getting around. NYC DOT has worked with a range of mobility providers, including several New York City-based companies, to bring innovative solutions to city residents in a way that works for New York City.

Since its launch in 2013, Citi Bike, a bike sharing initiative operated by Lyft, has seen over 110 million trips, installed over 1,150 stations across four boroughs, and maintains over 175,000 annual members.[035] The solar powered bicycle docking stations are internet-connected and users unlock bikes with RFID key fobs, the CitiBike smartphone app, or with a code from a station kiosk. Users can use smartphones to check for bike or dock availability and make payments. Citi Bike has changed how New Yorkers get around the city, and the network continues to grow into new neighborhoods. In 2019, Lyft announced a $100 million investment to expand the network, doubling the service area and tripling the number of bikes to 40,000.

In 2018, NYC DOT launched a pilot to bring "dockless" bike sharing to three service areas not served by the Citi Bike network - a model that uses GPS technology to allow bikes to be parked and picked up anywhere, without

[FIGURE 17 ▲] **Citi Bikes docked in their dedicated, connected stations.** *Photo: Anthony Fomin* the use of docking stations.[036] GPS connectivity allows users to locate and unlock a bike with a smartphone app, and may be used to keep bikes within a defined service area via a "geo-fence."[037]

In 2017, City Council passed Local Laws 47 and 50 requiring that the NYC DOT implement a carshare pilot program.[038] The two-year citywide pilot designated 285 parking spaces in municipal parking facilities and curbside in select neighborhoods for the use of carshare companies. Zipcar and Enterprise CarShare were selected for the pilot (Enterprise suspended its service in 2020) and the companies distributed vehicles across fourteen zones in four boroughs. Similar to bikeshare, cars can be found and unlocked via smartphone apps through the use of IoT technology – eliminating the need to rent a vehicle from a staff-managed rental location.

In 2018, NYC-based Revel added dockless electric moped sharing to the City's smart mobility options, offering these services to licensed motor vehicle drivers and using vehicles registered and licensed by the NYS Department of Motor Vehicles.[039] The project's rental model is similar to that used for dockless bikeshare or carshare. Starting service in Brooklyn and Queens, the company expanded its coverage areas, and grew its fleet to 1,000 mopeds in 2019 and 3,000 in 2020, in part to serve healthcare workers in need of transportation alternatives during the COVID-19 pandemic.[040] Revel uses geo-fencing technology to ensure vehicles are parked in designated service zones, and are not used on city highways or river crossings.[041]

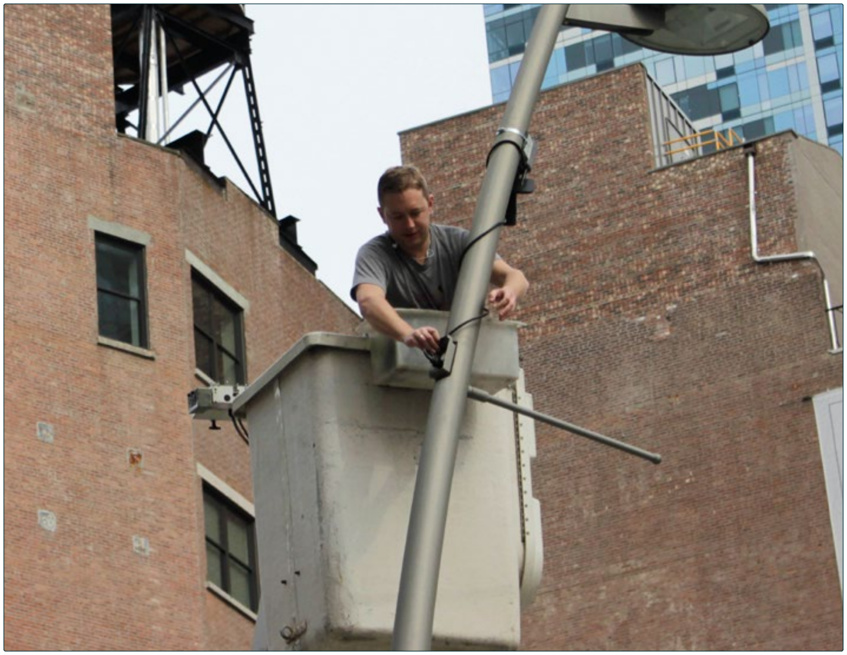
In 2021, NYC DOT will release a solicitation to conduct its first-ever pilot of electric e-scooters. The e-scooters are envisioned to operate similarly to the dockless bikes model.[042]

Real Estate Technology or Property Technology("PropTech") includes technology and innovations that transform the manner by which organizations design, build, exchange, operate, and use real estate, and is another area where IoT installations have been increasing across the city. The technology offers an extensive range of use cases, including options that increase efficiency and reduce energy usage – particularly salient as the demands of the climate crisis grow. Through the passage of local laws that make up New York City's 2019 Climate Mobilization Act, buildings must make significant reductions in their energy usage and subsequent greenhouse gas emissions.[043] Buildings larger than 25,000 square feet will specifically need to meet strict emissions limits starting in 2024, and they will be required to cut emissions by at least 40% by 2030. Leveraging technology opportunities such as smart thermostats, climate control sensors, connected heating and cooling devices like valves, plug-load management, and building management systems (BMS), buildings can reduce the amount of energy they consume and reduce their operating costs. Local companies like Perceptive Things (sensors for building management and maintenance) and Radiator Labs (energy efficiency for steam heat systems) are a part of the local ecosystem using IoT to improve building management and operations. [044]

In real estate and architecture, building owners and designers are applying IoT to understand how spaces are used. Either through internal technology development or through external providers, using IoT to measure occupancy and space utilization is becoming a new tool to design better, more comfortable spaces and increase efficiency. Amid COVID-19, it is being used to ensure social distancing between employees and analyze foot traffic patterns to ensure a safe return to offices. Companies like Gensler (architecture, design, and planning) and WeWork (co-working spaces) have developed related IoT technologies in their New York City offices in recent years and anticipate the data generated to impact their businesses moving forward.[045] The pandemic is also causing building owners and managers to reevaluate the air quality and flow inside their spaces. Connected air quality monitoring tools and related technologies might become more commonplace in the years to come.

New York City companies are also developing and innovating with IoT technologies directly. Latch, Canary, and Wink, for example, are developing a range of "smart home" products locally, such as smart locks, connected cameras, and hub platforms which illustrate that IoT is a component part of the local tech ecosystem. Local engineering and manufacturing company Adafruit Industries develops open-source hardware that is used by companies and individuals alike to develop next-generation products or to learn about and make their own IoT devices.

Since 2015, the New York City Economic Development Corporation (NYCEDC) has been supporting local tech companies – including those that develop or implement IoT – through the Urbantech NYC program by "securing flexible and affordable workspace, connecting innovators to one another, and promoting cutting-edge research."[046] The Urbantech Hubs, including New Lab and Company, give entrepreneurs space and resources to make an impact in the IoT ecosystem in New York City.[047] This year, NYCEDC and DCAS, in collaboration with the New York City Housing Authority (NYCHA), launched the PropTech Piloting Program, which seeks to leverage financial, intellectual, and technological capital from the PropTech industry and apply it to New York City's vast portfolio of publicly owned real estate. The program will foster the continued growth of IoT Proptech applications and promote equity in the sector by opening up significant swaths of non-luxury, non-Class A real estate for technology demonstrations. Additionally, in October 2020, the NYCEDC, and the NYC Department of Small Business Services (SBS), in collaboration with the Urban Tech Hub at Company (UTH) and CIV:LAB, launched the Neighborhood Challenge: Tech Forward program, an open innovation platform designed to crowdsource solutions to support the city's commercial districts and small storefront businesses that are facing severe impacts due to the COVID-19 pandemic.[048] This program could leverage a variety of IoT solutions to address challenges faced by small businesses such as retail, restaurants, personal care, and nightlife.



[FIGURE 18 ▲] **A noise sensor is installed through a collaboration between NYU CUSP and the Downtown Brooklyn Partnership.** *Photo: Downtown Brooklyn Partnership*

In 2017, NYCEDC also launched Futureworks NYC to foster the hardware startup ecosystem, help manufacturers adopt advanced technologies, and increase local production. The Futureworks Incubator program supported innovators and entrepreneurs develop new products, including IoT devices, that spanned industries with expert mentorship, workshops covering business and technical topics, and a hardware-focused community of supportive inventors and founders. The Futureworks Ops21 program made advanced manufacturing resources more accessible to local manufacturers by helping them learn about and adopt new digital manufacturing technologies including IoT.[049]

Community Organization Use

Various community groups are using and engaging with IoT in New York City today. Local business improvement districts (BIDs), such as Manhattan's Downtown Alliance and the Downtown Brooklyn Partnership, among others, have embraced IoT technology as part of their programming and support for local businesses. For several years, the Downtown Alliance has utilized pedestrian-counting technology to understand foot traffic in and around its neighborhoods, collecting and sharing data with businesses as well as the public. The Downtown Brooklyn Partnership has worked with the technology community in Brooklyn to demonstrate new technologies and use the space in Downtown Brooklyn as a "living lab," where it has monitored traffic flows and patterns and mapped air quality. In 2018, NYC CTO partnered with the NYC Department of Transportation, the Brownsville Community Justice Center (BCJC), and NYCEDC to launch its NYC[x] Co-Labs program.[050] A civic innovation initiative that combines community building, participatory research, tech education, and open innovation challenges to address urban inequality across NYC neighborhoods, Co-Labs works with communities to identify key challenges and co-design pilot technology programs to address them. In its inaugural project, the City and its partners worked to install interactive lighting on a section of Belmont Avenue in Brownsville, Brooklyn. The pilot aims to address community safety concerns about the Belmont corridor after dark. Through the addition of new lighting elements that respond to activity on the street, the project aims to boost resident sense of safety and increase nighttime use of the space.

The pilot's LED lighting elements are attached to City light poles and respond to movement on the sidewalk below by activating colored patterns up and down the block through wireless communication. These lights are not only digitally connected to each other but also to the internet, where data about when the lights are triggered is captured in a de-identified manner to help the City understand whether or not the lighting intervention is impacting pedestrian use of the street. The City and BCJC will combine these data with qualitative interviews with community stakeholders to understand the impact of the pilot intervention, and to identify next steps.

Notably, the project uses "privacy by design" principles in its collection of data. During the project's initial engagement and co-design process, community members expressed concern about adding surveillance elements to their neighborhood. For this reason, technology that cannot identify individual attributes was intentionally chosen. The passive infrared sensors used merely detect the "heat signature" of a person or persons, and they can only differentiate between living and inanimate objects. This ensures that the data collected are the minimum amount needed to understand time and quantity of foot traffic along the corridor.

Looking forward, the NYC[x] Co-Labs program will be piloting another IoT project in 2021 as part of a "Housing Rights Challenge" in Inwood and Washington Heights. NYC CTO, working with the Department of Housing Preservation and Development, NYCEDC, and the Mayor's Office to Protect Tenants will partner with Heat Seek, a New York City-based technology non-profit that creates low-cost, web-connected temperature sensors that help tenants prove and resolve illegal and sometimes life-threatening lack of heat in their apartments during cold winter months. Heat Seek installs proprietary temperature sensors and offers technical expertise to assist tenants in documenting landlord failures to provide adequate heat, in an effort to restore that right through advocacy.

Finally, in April of 2018, the National Science Foundation (NSF) announced a $22.5 million grant to a set of local partners as part of its Platforms for Advanced Wireless (PAWR) program. The so-called COSMOS project, led by Rutgers University, Columbia University, and New York University, in partnership with the City of New York, City College of New York, University of Arizona, and the community-based organization Silicon Harlem, has the goal of deploying "an advanced wireless research testbed in West Harlem with a technology focus on ultra-high bandwidth and low latency wireless communication tightly coupled with edge computing."[051] When completed, the testbed will consist of 40-50 advanced software-defined radio nodes along with fiber-optic front-haul and back-haul networks and edge and core cloud computing infrastructure. This testbed will push advancements in wireless technology but also will be used for research on smart city and IoT applications. The testbed is just one of two like it in the United States and is a testament to New York City's commitment to advanced research and forward-thinking position within the field of IoT and wireless technologies.

As outlined below, libraries and other community organizations are also working to train New Yorkers to use and interact with IoT across society.

Local Governance and Coordination

In recent years, City legislation has increased the City's capability to respond to the opportunities and challenges of using connected technology. As mentioned, the NYC3, established by Executive Order in 2017 and incorporated into the City Charter in 2020, is establishing an IoT security assessment capacity for the City, as well as IoT cybersecurity policy, standards, and guidance for agencies. Also in 2017, the New York City Council passed Local Laws 245 and 247, which together established the role of Chief Privacy Officer, a citywide privacy protection committee, and a new privacy protection framework in New York City.[052] In 2018, the Mayor issued an Executive Order that established the Mayor's Office of Information Privacy (MOIP).[053] The CPO leads MOIP, working to "protect the privacy of New Yorkers' identifying information, while maximizing data sharing across agencies where permitted by law," working through a set of Citywide Privacy Protection Policies and Protocols, established in 2019.[054]

Additionally, the City enacted its Open Data Law in 2012, established the Mayor's Office of Data Analytics (MODA) in 2013, and enshrined it in the City Charter in 2018, with a mission to apply "strategic analytical thinking to data to help city agencies deliver services more equitably and effectively and increase operational transparency."[055] As the City's data collection and use expands in quantity and diversity of mode, MODA plays a crucial role in managing and making sense of it. MODA works with DOITT to oversee the NYC Open Data program, a broad effort to make data from City agencies and their partners more publicly available, and to engage communities in making use of it. MODA further supports city agencies in sharing data not suited for public release due to its sensitivity by contributing to

ONLINE
You Are Safe !
Device Safety
Network Safety
App Safety
145 Checks Last Week
Danger Zone
THE Sole Objective for Persistent Foothold
The Primary Mechanism for Targeted Attacks
Untargeted, Advertising & Fraud Threats
Device Attacks
Network Attacks
Global Internet Co
NYC SECURE
PROTECTING NEW YORKERS ONLINE

[FIGURE 19 ▲] Mayor Bill de Blasio, joined by the head of NYC Cyber Command and other stakeholders, announces a new cybersecurity initiative.
Photo: Mayoral Photo Office

technology system requirements and pursuing improvements to City's data sharing platforms and tools. Finally, MODA offers agencies support in analyzing their data toward making meaningful use of it, via short- and long-term analytics collaborations, and by convening agency analytics professionals to support City capacity. Internal coordination, data sharing, and building/maintaining internal capacity to make use of data are critical to maximizing the City's use of IoT resources.[056]

In 2019, the City created the position of Algorithms Management and Policy Officer through an Executive Order and mandated the development of a framework for the fair and responsible use of algorithmic tools by City agencies, which can come into play in certain IoT deployments.[057]

In 2018, New York City joined Barcelona and Amsterdam in founding the Cities Coalition for Digital Rights, a network of municipalities and multilateral organizations that is dedicated to "eliminating impediments to harnessing technological opportunities that improve the lives of [their] constituents, and to providing trustworthy and secure digital services and infrastructures that support [their] communities."[058] The Coalition is founded on the belief that "human rights principles such as privacy, freedom of expression, and democracy must be incorporated by design into digital platforms starting with locally-controlled digital infrastructures and services."

It has committed to five major, "evolving" principles:

→ 1 Universal and equal access to the internet, and digital literacy,

→ 2 Privacy, data protection and security,

→ 3 Transparency, accountability, and non-discrimination of data, content and algorithms,

→ 4 Participatory democracy, diversity and inclusion, and

→ 5 Open and ethical digital service standards.

The work of the Coalition is supported by the United Nations Human Settlements Program (UN-Habitat) and includes sharing best practices, learning from other cities' challenges and successes, and coordinating common initiatives and actions. As the work of the Coalition covers all aspects of digital rights, this includes the use of IoT systems and the data derived from them.

Local Public Education, Training, and Workforce Development

Several City-run or City-funded digital literacy providers offer training in the use of consumer IoT products.[059] For example, in addition to offering various lectures and training programs that review the use of IoT in "smart cities," "smart homes," healthcare, and other areas, Older Adults Technology Services (OATS) – a service provider under contract with the NYC Department for the Aging – delivers direct instruction and support on using consumer IoT devices such as smart speakers and activity trackers in a number of senior centers across the city.[060] Older adults learn to use activity trackers to monitor their fitness levels in OATS exercise programs, for example, or to use smart thermostats as a tool to save money and balance their household budgets in classes on financial literacy.

City-run providers also offer public data literacy or physical computing training – skills that are foundational to participating in the broader IoT ecosystem. The Mayor's Office of Data Analytics has partnered with the civic technology group BetaNYC and City institutions to advance data literacy and provide training on the use of the NYC Open Data portal. Among these efforts is a collaboration with BetaNYC and the Queens Public Library to train a corps of volunteer "Open Data Ambassadors" who, in turn, have led data literacy programs at library branches in every Queens community board, engaging with community-specific data to support technical skill development and civic engagement. Several City providers also offer physical computing programs.[061] In the summer of 2019, the Queens Public Library's Tech Lab rolled out an eight-week Community Science Project that, among other activities, used Airbeam sensor kits to monitor air quality in the community, and identify pollution hotspots.

Digital literacy providers across the city also offer training and support in online privacy and data security. Notably, in 2018, the City rolled out its NYC Digital Safety initiative, which has worked to train staff at every branch library in the city to answer patrons' questions about online privacy and security.[062]

The NYC Department of Education also offers foundational computational thinking and computer science education, including physical computing for K-12 students. In 2015, New York City launched its CS4All initiative, which aims to bring Computer Science education to every elementary, middle, and high school by 2025, with an emphasis on female, Black, and Latino students. The NYCDOE currently provides multiple curriculums across all grade bands, including physical computing curriculum for middle schools, in which students learn to program interactive hardware.[063] It uses simple, programmable computer devices such as the micro:bit and Arduino to let students make interactive machines. Teaching physical computing is a first step to teaching students about connected devices.

The previously mentioned COSMOS project and testbed in Harlem also includes an educational component that features IoT topics. The COSMOS Education Toolkit offers a

Climate, Sustainability, and Resiliency

IoT can play an important role in addressing climate change, promoting sustainability, and ensuring resiliency for people and their livelihoods. In mobility and transportation, IoT has opened up new possibilities for vehicle sharing, helping residents in cities all over the world transition to cleaner forms of transportation like bicycles, electric scooters, and electric cars. Connected technology will also help owners of electric vehicles find available charging stations more easily, making the transition from internal combustion vehicles smoother and less burdensome. In energy production and building efficiency, renewable energy output can be monitored in real-time and load demand can be managed accordingly. Buildings are being made "smart" through the use of sensors and connected management systems to adjust the use of heating and cooling systems to optimize energy use. In public spaces, sensors are being used to monitor air pollution, flood events, heat conditions, and other health and safety risks that can help with adaptation and addressing the root causes of environmental issues. IoT is also paving the way for growth in "controlled environmental agriculture" (CEA) which allows spaces like warehouses to be converted into farms where crops are closely monitored for optimal light, humidity, water, available CO2, and nutrient conditions. The long-term impacts of this are not yet known but moving the source of food production closer to residential hubs reduces emissions from transportation as well as the environmental impacts of fertilizer use. As cities and countries continue to realize the importance and immediate need for climate action, the role of IoT will continue to grow and serve as a tool to fight climate change and make our cities and world more sustainable and resilient for years to come.

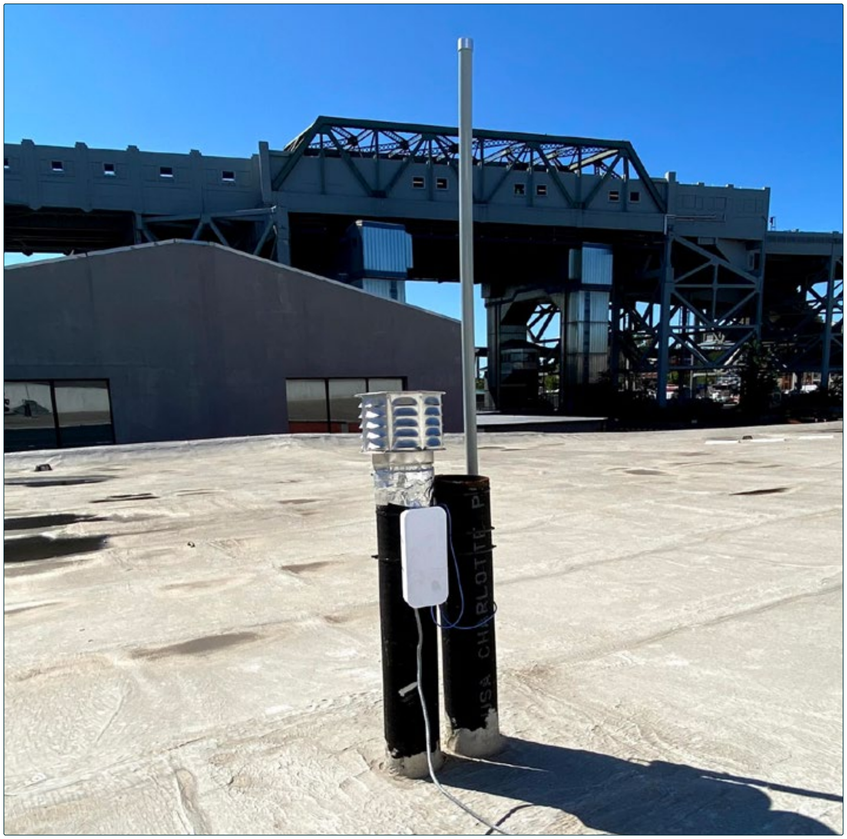
curriculum that “blends the three disciplines of mathematics, science, and computer science into a seamless package that helps prepare students to be competitive in an evolving, international workforce.”[064] There are currently a total of 125 experiments available through this resource, for students ranging from sixth to twelfth grade. The toolkit includes hardware called the ”IoT Node“ which is comprised of a ”microcontroller based device with various wireless interfaces (i.e., XBEE, Wi-Fi, and Bluetooth), and sensing capabilities such as air and soil temperature, humidity, light luminosity and color, carbon dioxide (CO2) levels, dust (PM1.0, PM2.5, and PM10), noise sensor, and accelerometer.”[065] The COSMOS team has trained educators throughout New York City to teach from its curriculum and engage students with lab projects like air quality monitoring, understanding how radio waves travel around obstacles, monitoring plant growth, and more.

Finally, the City University of New York launched a Building Performance Lab (“BPL”) in 2006, dedicated to “supporting the sustainability of the built environment through research, continuing education, and industry collaboration.”[066] Among the initiatives undertaken by the BPL is a workforce education program aimed at upskilling building managers and engineers to use, among other technologies, IoT and IoT-derived data to manage building systems, and support energy efficiency.[067] BPL has historically offered this training to private sector stakeholders. Since 2009, DCAS has worked with BPL and CUNY’s School of Professional Studies to coach its own workforce through a joint educational initiative called the Energy Management Institute (“EMI”). Aimed at the breadth and depth of efficiency learnings and data management, EMI has trained over 2,500 unique City employees since its launch.

Future Outlook

As IoT develops it is rapidly becoming more accessible across sectors, as awareness and usability grow. Technical advances on the horizon promise to expand IoT's capabilities, applications, and adoption.

One important area of advancement will likely be in the field of communications networks and connectivity. 5G, Narrow Band IoT (NB-IoT), and LoRaWAN are all growing in their coverage which will make connecting devices easier and, in the case of 5G, improve performance and capabilities. 5G, with its low-latency and high bandwidth, promises to enable new applications in areas like connected vehicles and energy management. LoRaWAN and NB-IoT networks enable sensors to connect to networks over greater ranges and their low-power capabilities allow for smaller, lower-cost, and more discreet devices to be deployed on battery power, which can make environmental monitoring and other applications easier to pursue.


[FIGURE 20 ▲] A LoRaWAN gateway and antenna installed by NYU on a roof in Gowanus, Brooklyn. *Photo: NYU CUSP*

As network capabilities are advancing, so are the hardware devices that are at the core of IoT. Computing power on microcontrollers and single-board computers continues to improve, allowing devices to become simultaneously smaller and more powerful, which can make for more wearable and mobile applications. The increase in computing power also lays the groundwork for more data processing to be performed on the IoT device itself, rather than on a server located somewhere else. This so-called "edge" computing reduces the amount of data that needs to be transmitted over the internet, saving bandwidth and preserving privacy. This more powerful edge computing also enables an increase in the amount of machine learning and artificial intelligence processing that can be done on IoT devices. For example, applications involving analyzing patterns in data (the sounds emitted by an industrial machine) can help to automate decision making (turning off a machine that doesn't sound right) and send notifications to a supervisor right from the device. By doing the processing on the device, they are saving bandwidth and reducing latency by not sending data to the cloud for processing.

New hardware devices are also being designed to consume significantly less power, which allows for applications without a connection to the electrical grid, either from battery power, solar energy, or other renewable source making devices capable of being deployed in an increasingly varied number of locations. This is especially true for environmental sensing where large numbers of sensors are needed, often in locations where electrical grid-connected power is not accessible or neither convenient nor cost effective to access.

Wearable devices are also becoming more capable. Fitness trackers and smart watches now have the ability to do electrocardiograms (ECG), read heart rates and temperature, monitor electrodermal activity and blood oxygen level, as well as track sleeping patterns. In the future, monitoring blood pressure, dehydration, blood glucose levels[068] and other vital signs will be commonplace as well. As called out in the section detailing IoT and COVID-19 response, wearables are being used in new ways to monitor health and wellness.

Another critical piece of the future of IoT is the increased use of machine learning and artificial intelligence (AI). The difference between a "connected" device and a "smart" device is its ability to process data and make decisions or suggest actions based the information it creates. Artificial intelligence and machine learning can be implemented in a number of ways to process large amounts of data and pull insights out of them. For example, fleet vehicles outfitted with diagnostic sensors and telematics allow a fleet owner to monitor vehicle performance and predict maintenance needs before the symptoms emerge or optimize routes to reduce the number of vehicles needed at a given time. AI is also being used in energy management applications where sensors and heating or cooling systems work in tandem to monitor usage and occupancy patterns and maintain thermal comfort while also reducing energy usage.

These advances are already here today but will become more prevalent in the coming years, making IoT more relevant, accessible, and useful.

The Strategy

Opportunities and Challenges for New York City

Integration of any new technology brings both opportunities and challenges. This section outlines some of the key insights from NYC CTO's stakeholder interviews across the New York City IoT ecosystem – focusing attention on the key opportunities and challenges IoT brings for New York City government, residents, community groups, and businesses.

Government

As noted, IoT presents numerous opportunities for New York City government, allowing the City to increase the efficiency of systems, improve services, enhance security, add transparency, and better advocate for change.

To support these gains, there is opportunity for the City to boost agencies' knowledge about IoT and their capacity to utilize it. Even agencies with traditional IT support can benefit from developing the skills and tools needed to deploy and manage emerging IoT technology. Additionally, there is opportunity to support agencies to test and experiment with new technologies or methods of implementation – an important tool for proving the value of emerging technologies like IoT.

External partnerships across academia, industry, and community organizations can be immensely valuable to the City's ability to use IoT to meet its needs and serve residents. Clear and accessible information about the City's needs and available avenues for collaboration can help support the development of these partnerships.

When collaborating with academic and industry partners, having a test site for new technologies and research can accelerate collaborations and results. To this end, many cities have benefitted from having a "testbed" or "living lab" location where there is existing infrastructure for wireless communication, power access, and general access agreements that can reduce the planning and approval steps required every time a product or research idea is tested.

While certain types of data must be kept private, there is opportunity for City agencies to share more non-restricted data, expand impact, and produce greater transparency. Today, there is opportunity to support broader sharing of real-time data from City IoT deployments, making it accessible beyond the agency or group that has deployed devices, where appropriate. Sharing data in this way can boost its utility and increase both efficiency and transparency.

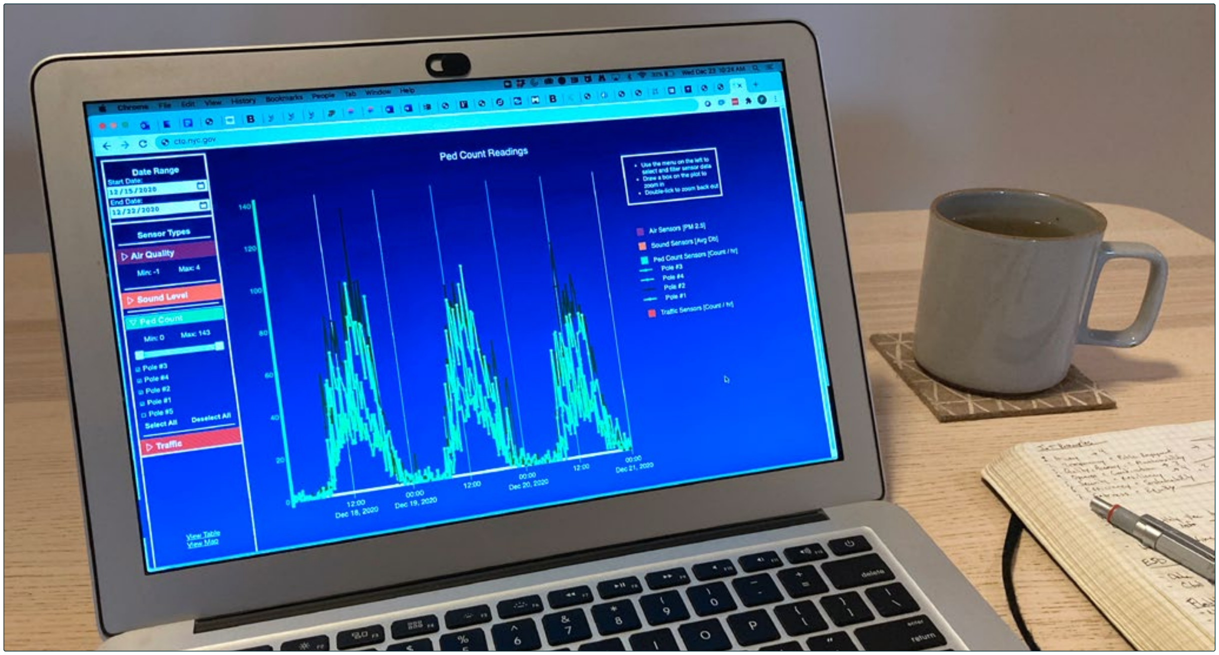
Finally, there is opportunity to build on the City's efforts to coordinate IoT use to ensure efficiency and interoperability, and support consistency in approach to privacy, cybersecurity, transparency, public engagement, and equity. As noted, the City's Guidelines for the Internet of Things, and the NYC IoT Strategy represent major steps forward in organizing the City's approach to IoT. Standard, citywide procedures will further support consistency in how these important aspects of City IoT deployments are handled.

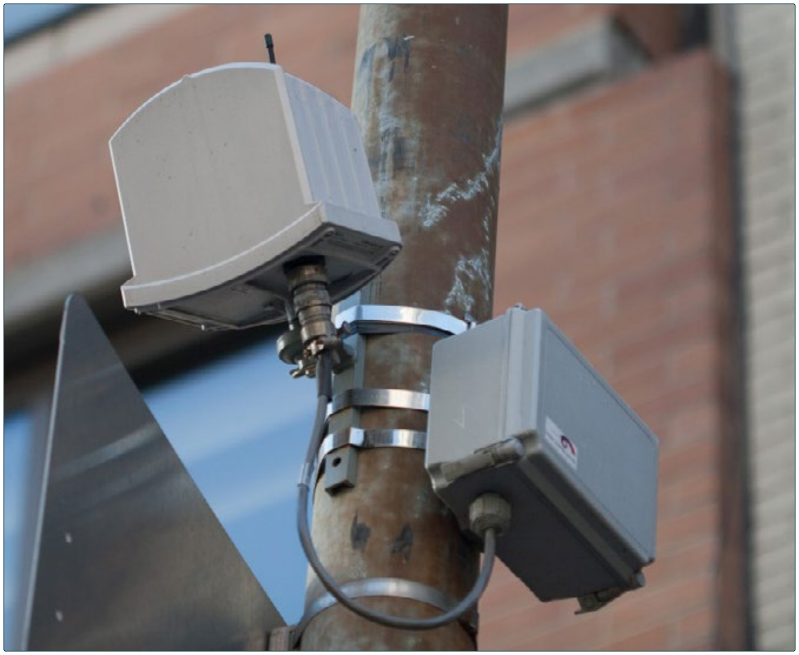
Residents

From the perspective of New Yorkers, consumer IoT products can boost health and wellness, offer reduced costs and energy savings, and make life more convenient. Industry and government applications can improve the quality of the products and services residents use or make them cheaper. They can make workplaces and communities safer and more sustainable, or present new work opportunities. They can support civic engagement, and public involvement in product or service design, or decision-making.

There are also, as noted, a number of challenges residents might face as they interact with IoT across sectors. On the one hand, IoT integration is broadly generating an ever-increasing amount of data about New York City residents, and the world around them. Much of this data are generalized, but some are more individualized, raising concerns about privacy and data security. Residents may also see inequitable benefits or harms due to the way IoT has been designed, deployed, or utilized across society.

City residents may, for their part, have limited knowledge about IoT technology or a limited understanding of what data about them are being collected and what risks exposure of such information to unauthorized persons or entities might carry. Residents may also be unaware of how and where IoT is being used across the city. Lack of understanding or lack of transparency can lead to mistrust of the technology or the organization deploying it. It can also leave New Yorkers more vulnerable to having their data misused – a risk that may disproportionately impact certain vulnerable populations, such as survivors of domestic violence, and can compound any instances of disempowerment or harm experienced from





[FIGURE 21 ▲] Data presented through the IoT Data Dashboard prototype created by NYC CTO.

[FIGURE 22 ◀] A NYC Department of Transportation traffic lane sensor in midtown Manhattan. *Photo: Mayo Nissen* other sources. Where access to IoT data or resident data literacy is more limited, New Yorkers may not have meaningful opportunities to provide input or be involved in IoT-related decision-making. Finally, New Yorkers may lack technical knowledge or skills needed to adapt to IoT being integrated in their workplaces, or those workforce skills that will be prioritized in the future.

Businesses and Community Organizations

Currently, there are few global standards, best practices, and policies that have been developed to support IoT interoperability or ethical use. Organizations of all types can benefit from this kind of policy and standards development, to the extent that it helps them to more effectively use IoT and realize the technology's full potential. This is a significant and highly complex undertaking, as companies have differing – and sometimes competing – interests. However, improving the ecosystem has the potential to expand the market for IoT, and make existing investments more productive. Industry taking initiative to institute standards can also reduce the need for governments to legislate, which some companies might prefer. There is opportunity to support public-private exchange and partnership in support of these measures, and toward more broadly advancing the City's principles and goals, as detailed in this IoT Strategy.

There is evidence that internationally, businesses face current and projected unmet workforce need for IoT/data-related skills.[069] There is opportunity in New York City to conduct further engagement with industry stakeholders to better understand their needs in this regard, and to work to connect local talent to meet them. There is also opportunity to support a thriving and fair local IoT economy in sourcing technology and talent for City IoT initiatives.

IoT can also offer community-based organizations (CBOs) opportunities to streamline operations and reduce costs, better understand and quantify local issues with data, and offer communities information and skills. While many CBOs lack the technical skills to take on this work themselves, by collaborating with New York City government and other community groups, they might leverage the technology and the data it produces. Many New York City business improvement districts (BIDs) are already doing this kind of resource sharing, often alongside government counterparts. By collaborating on technology projects and mutually sharing collected data, BIDs and City government can expand their knowledge and better utilize their resources. There is also opportunity for greater collaboration across sectors to inform the education, training, and advocacy community groups perform, and help ensure residents are empowered in their interactions with IoT as consumers, residents, and workers.

Recommendations for a Healthy IoT Ecosystem in NYC

Based on its research, pilots, and goals, the City puts forward the following recommendations toward promoting a productive, responsible, and fair IoT ecosystem for New York City government, businesses, community groups, and residents.

Government

While New York City has made great strides in integrating IoT technology, producing broad and diverse benefits, there is still room for improvement to the City's approach. The following recommendations outline how the City will keep improving the use of these technologies for its own operational effectiveness and for the benefit of all New Yorkers.

Capacity Building

City agencies can best utilize IoT when they have up-to-date information, and when experience and tools are shared across organizations. To foster this intra-city communication, the City should develop a knowledge base and culture of sharing IoT resources and best practices:

- Establish a Smart City Collaborative for City agencies comprised of an "Opportunity Network" to share information and collaborate on new smart city opportunities and a biannual IoT Forum to support coordination and knowledge sharing on an ongoing basis
- Develop an internal City consultancy and office hours program to provide support for developing City IoT projects and opportunities
- Grow NYC CTO's "Rapid IoT" program that enables agencies to demonstrate the utility of IoT technology quickly and cost-effectively, and prove the case for scaling where appropriate

Innovation

The City has a need to take advantage of the latest technology, which requires an enhanced level of responsiveness to emerging challenges and emerging solutions. The City should advance its use of IoT by exploring emerging technologies, as well as novel implementations and deployments:

- → Continue to test new sensing and power technologies, approaches, and infrastructure through pilot or challenge-based programs
- → Establish a municipal "testbed" location to quickly and efficiently pilot new technologies in real-world conditions
- → Support the development of IoT wireless communications networks to facilitate ease of deployment
- → Pursue new research opportunities and collaborations

Partnerships

The City can help ensure potential partners in academia, industry, and the broader community have clear paths to engage with the City to demonstrate the efficacy of new technologies:

- → Foster partnership opportunities with academic institutions, industry, and community-based organizations
- → Establish a continuous pilot program framework within the aforementioned "testbed" to assess new technologies on a rolling basis, without requiring topic-specific calls for innovation

Data Sharing

By establishing new data-sharing mechanisms, the City can minimize duplicate IoT device deployment and data collection, maximize productive use of data across government agencies, and provide New Yorkers the opportunity to directly access, utilize, and respond to non-restricted data:

- → Accelerate efforts to establish a near-real-time IoT data platform for agencies and the public

Coordination and Oversight

Coordination and oversight are essential to ensuring City IoT deployment is efficient, secure, interoperable, and that it protects New Yorkers' digital rights. The City should continue to work through the IoT Working Group to:

- → Update and maintain an internal inventory of City IoT devices, on a continual basis
- → Establish a standardized device review process, in coordination with agency stakeholders, that includes equity, security, and privacy oversight
- → Create broader standards and procedures for City IoT deployments, including processes for working with City infrastructure owners as well as standard public engagement and transparency measures

Residents

The City can play an important role in ensuring residents are informed and engaged in how IoT is used across the city, and how it might be impacting their lives and communities. Moreover, as IoT takes on a larger role in everyday life, New Yorkers should be equipped with information and skills to be empowered in their interactions with emerging technology, and to take advantage of the opportunities it brings.

Public Awareness, Education, and Training
The City can work to educate the public on IoT benefits, risks, and best practices:

- → Publish accessible information on the state of connected technology, including both the benefits and the risks to residents, such as those related to privacy, security, fairness and equity
- → Work with local digital literacy providers to coordinate training on consumer IoT, privacy, data security, and data literacy
- → Identify opportunities across education and training providers to support access to IoT tools and information, such as connectivity and access to City data and initiatives
- → Create a public Smart City Catalog of projects and pilots from across the City to share successes and developments with the public, non-profits, and other city governments

Transparency and Accountability
The City can work to ensure residents have visibility into how IoT is being used across the city, and offer them opportunities to provide input or express concerns:

- → Develop and deploy public notices of IoT use in public space
- → Offer mechanisms for public input before, during, and after long-term City IoT deployments

Workforce Development
In order to foster equitable participation in the IoT ecosystem and economy, the City should take action to support IoT skill-building and workforce participation:

- → Work to explore local IoT workforce needs among employers, including those related to distinct IoT jobs and existing jobs in which IoT is a supplemental skill set, and identify ways to integrate appropriate IoT skills into City training opportunities
- → Work across agencies to identify opportunities to support local hiring for City IoT work, where practicable

Policy, Advocacy, Legislative and Regulatory Action
As a metropolis of more than 8 million people, the City can influence the choices of private actors in a variety of ways.[070] The City can engage with companies that use or make IoT technology to articulate its positions and

[FIGURE 23 ▲] New Yorkers on the street of lower Manhattan. *Photo: Arthur Osipyan* policies and can recognize good actors – to the benefit of residents:

- Foster dialogue between government and industry
- Support certification efforts that allow companies that are using industry best practices to be acknowledged for their good work, enabling New Yorkers to make better informed decisions
- Track and pursue opportunities to advocate for state and federal legislation that aligns with City IoT goals, as outlined in this IoT Strategy

Businesses and Community Organizations

As noted above, private companies have multifaceted influence on New York City's IoT ecosystem, using the tech for their own business purposes, developing and selling the products and services used across sectors, and employing New Yorkers to deliver all of the above. Additionally, community groups such as BIDs and non-profits use IoT themselves, partner with the city, and employ public data to support their work. Community groups further work to support public engagement in IoT projects and to educate the public about its use and impact across society. The City can take steps to support private-sector and non-profit

[FIGURE 24 ▲] Young people participate in a workshop hosted by NYC[x] Co-Labs.

approaches and actions that benefit New Yorkers.

Industry Policies, Standards, and Best Practices
To better protect and support consumers, and maintain trust, companies should develop and adopt internal ethical standards and policies, built upon industry best practices. The City can play a role in supporting these measures in its engagements with industry:

- ➔ Establish a structure for regular communication between government and industry
- ➔ Encourage companies to develop internal policies for how they collect, manage, use, share, and store data that incorporate ethical and digital rights considerations, such as using "privacy by design" approaches, or requiring "opt-in" user settings related to use of personal data, where applicable
- ➔ Encourage companies to create plans for the continuity of their products' operations even in the event their company is no longer able to provide support, either through interoperability standards, open sourcing initiatives, or third-party support

Local Sourcing
Supporting local companies that offer IoT products and services provides a boost to New York City's economy and workforce; choosing Minority and Women-owned Business Enterprises (M/WBEs) supports equitable participation in the IoT ecosystem.[071] The City should look for opportunities to employ local and M/WBE vendors in its IoT procurements:

- ➔ Identify opportunities to support local and M/WBE product sourcing for City IoT needs, where practicable

Collaboration for Community Benefit
There is opportunity for the City and community groups to collaborate to deploy technology that is used for the good of the community, support public awareness of IoT use, and share data toward greater engagement.

- ➔ Establish structures for regular communication between government and community groups to ensure mutual awareness of IoT projects and data, support alignment in approaches, and increase the capacity of community groups to use IoT and associated data to support their work
- ➔ Work with community-based organizations to support engagement with residents about the use of IoT in communities
- ➔ Facilitate data sharing between the City and community groups, to allow government, organizations, and residents to easily make use of available resources

Next Steps

In order to fulfill the recommendations outlined above, the City will take the following steps in 2021-22.

Foster Innovation

- → Launch a Rapid IoT data collection program
- → Develop a municipal "testbed" and launch a continuous pilot program framework to utilize it, subject to City procurement rules
- → Test new technologies and approaches through pilot or challenge-based programs

Promote Data Sharing and Transparency

- → Establish scope and resources for citywide IoT data dashboard
- → Launch a Smart City Catalog to publicly share information about City projects
- → Solicit community feedback on the NYC IoT Strategy, and work to incorporate it
- → Report annually on the City's progress toward reaching its IoT goals.

Improve Governance and Coordination

- → Launch a Smart City Collaborative, and a biannual IoT Forum for City agencies
- → Establish an internal City consultancy and office hours program
- → Coordinate wireless IoT communications network deployments across City projects, to support expanded availability for future City deployments
- → Establish a Citywide IoT device inventory
- → Implement a standardized and comprehensive device review process, in coordination with agency stakeholders
- → Develop, in collaboration with the City's Chief Privacy Officer and other partner agencies, new standards, policies, and procedures for City IoT deployments; test implementation of privacy and equity impact assessments and newly developed signage to support IoT transparency in pilot projects already underway

Derive Value from Cross-Sector Partnerships

- Establish and promote an online channel for expressions of interest in collaboration – for academic, community, and industry partners, subject to City procurement rules
- Pursue grants and research partnership opportunities that align with the City's needs and goals

Engage with Industry and Advocate for Communities

- Conduct research to better understand the need for IoT skills among local employers
- Work with City digital literacy and workforce training providers to coordinate IoT-related training, or integrate IoT-related skills into training opportunities, as appropriate
- Contribute on an ongoing basis to private sector norm-setting by communicating the City's position on industry policy, standards, and best practices Identify opportunities to leverage City procurement or regulatory authority to support the City's positions on industry policies, standards, and best practices, and to support local hiring and local and M/WBE sourcing for City projects
- Advocate at the state and federal levels legislation aligned with City goals.
- Establish an annual forum for industry and community partners on IoT usage.

The City welcomes ideas and suggestions in response to the content of the NYC IoT Strategy, at: https://our.cityofnewyork.us/a/iotstrategyfeedback

Glossary of Terms

Biometric data
body measurements and analysis related to a person's unique physical characteristics often used for personal identification and access control in digital systems.

BLE radio
a low-power radio protocol that uses the 2.4Ghz frequency band and used in both consumer and industrial applications.

Brute Force Attack
a cyber-attack consisting of trial-and-error attempts to guess a password.

Denial-of-Service Attack
a cyber-attack whose intent is to make a machine or network resource inaccessible for its intended users by disrupting service through the internet by bombarding the target with traffic.

Gateway
a hardware device that connects networks together using more than one communications protocol.

Geo-fence
a virtual perimeter, as defined in software, for a physical geographic area and is used to trigger an action when a device (GPS, RFID, Wi-Fi, cellular) interacts with the perimeter.

LoRaWAN (Long-Range Wide Area Network)
a low-power, wide-area networking protocol designed for wireless communication between IoT devices using open LoRa technology.

NB-IoT (Narrowband Internet of Things)
a low-power, wide-area networking protocol designed for wireless communications between IoT devices using licensed LTE technology.

Penetration test
colloquially known as a *pen test*, *pentest*, or *ethical hacking*, is an authorized simulated cyber-attack on a computer system, performed to evaluate the security of the system.

Personally Identifiable Information (PII)
any data that could potentially identify a specific individual.

RFID (Radio Frequency Identification)
a method of identifying objects or "tags" using electromagnetic fields. A RFID tag contains a radio transmitter and receiver that can be "read' by another device. Tags can be passive or active, which affects their range and possible use-cases.

Smart City
a local government utilizing technology and planning practices to generate better outcomes for its residents through the use of data.

Telematics
an electronic system used to track the location of a vehicle along with other vehicle attributes such as speed, braking, idling, and fuel consumption among others.

Wayfinding
a means of orienting oneself in physical space and/or navigating from one point to another.

Endnotes

001 E.g.: Statista *"Number of internet of things (IoT) connected devices in 2018, 2025, 2030,"* (May, 2019) at https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

002 The term "smart city" may be used to describe a broad array of efforts, including work to ensure access to and adoption of high-speed or "broadband" internet, integration of a wide range of established and emerging technologies in support of efficiency, sustainability, health, safety, cost efficiency, economic growth, equity, and quality of life, among other goals, as well as non-technical projects that use innovative approaches to meet these goals.

The City's "Internet Master Plan" was released in January, 2020, and can be found at: https://nyc.gov/internetmasterplan.

The City's broader OneNYC 2050 strategy, which includes varied initiatives in this category, can be found at https://onenyc.cityofnewyork.us/.

003 NYC CTO's name in 2015 was the *Mayor's Office of Technology and Innovation (MOTI)*. The report is available at https://www1.nyc.gov/assets/forward/documents/NYC-Smart-Equitable-City-Final.pdf

004 The Guidelines are available at https://iot.cityofnewyork.us/.

005 The City codified its approach to "digital rights" in 2018, joining Barcelona and Amsterdam to found the Cities Coalition for Digital Rights, a network of municipalities and multilateral organizations dedicated to "eliminating impediments to harnessing technological opportunities that improve the lives of [their] constituents, and to providing trustworthy and secure digital services and infrastructures that support [their] communities." More on the Coalition and the principles it has outlined is included below and is available at https://citiesfordigitalrights.org/.

006 For more on the AMPO, see https://www1.nyc.gov/site/ampo/index.page.

007 See, e.g., Schwartz, Eric Hal, *"The 4 biggest controversies for voice assistants in 2019,"* Voicebot.ai (December 31, 2019) at https://voicebot.ai/2019/12/31/the-4-biggest-controversies-for-voice-assistants-in-2019/. and Shaban, Hamza, *"An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts report says,"* Washington Post (May 24, 2018) at https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/.

008 In response to these revelations, many voice assistant manufacturers changed their policies on access to voice data, including allowing users to opt out of human reviews or to control who has access to recordings

for product improvement purposes. E.g., Newman, Lily Hay, *“Google Tightens Its Voice Assistant Rules Amid Privacy Backlash,“* Wired (September 23, 2019) at https://www.wired.com/story/google-assistant-human-transcription-privacy/.

[009] See https://data.melbourne.vic.gov.au/stories/s/visualisations/aqrs-eqqs/.

[010] See http://www.pedestrian.melbourne.vic.gov.au/#date=28-09-2020&sensor=Col15_T&time=13.

[011] For more on these Copenhagen, Helsinki, and Las Vegas initiatives, see https://cphsolutionslab.dk/en/projekter/labs, https://fiksukalasatama.fi/en/, and https://innovate.vegas/Portals/innovate/Documents/Innovation%20District%20Factsheet-%20FINAL%20-%209-18-18.pdf?ver=2019-01-23-112339-113, respectively.

[012] For the full text of the Act, see https://www.congress.gov/bill/116th-congress/house-bill/1668/text.

[013] For the full text of the Bill, see https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

[014] The ordinance defines “surveillance” as *“observ[ing] or analyz[ing] the movements, behavior or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”* For the full text, see https://library.municode.com/wa/seattle/ordinances/municipal_code?nodeId=917005.

[015] Ibid.

[016] For the full text of the Act, see http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Note that, as the State’s website indicates there are “many exceptions” to the “right to delete” provision, see https://oag.ca.gov/privacy/ccpa#sectione.

[017] For more information, see https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[018] For more information, see https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm and https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/06/1493-S.SL_.pdf, respectively.

[019] For the full Procedures document, see https://www.derbyshire.gov.uk/site-elements/documents/pdf/working-for-us/data/gdpr/privacy-impact-assessment/privacy-impact-assessment-procedures.pdf.

[020] For more information, see https://gdpr.eu/.

021 *“The NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,”* U.S. Department of Commerce, National Institute of Standards and Technology (January 16, 2020) at https://www.nist.gov/privacy-framework.

022 Ibid.

023 For more information on the DOT’s *Real Time Traffic Information* project, see https://flowmap.nyctmc.org/midtown_map/index.html and https://www1.nyc.gov/html/dot/html/about/datafeeds.shtml#realtime; on cyclist counting, see https://www1.nyc.gov/html/dot/html/bicyclists/bike-counts.shtml; on energy use tracking, see https://data.cityofnewyork.us/City-Government/DCAS-Managed-Building-Energy-Usage/ubdi-jgw2; on water main maintenance, see https://www1.nyc.gov/site/dep/news/20-032/new-york-city-registers-fewest-water-main-breaks-since-record-keeping-began.

024 This project was detailed in the City’s 2015 publication, *“Building a Smart + Equitable City,”* which is available at https://www1.nyc.gov/assets/forward/documents/NYC-Smart-Equitable-City-Final.pdf. For more on the initiative, see https://www1.nyc.gov/site/dep/pay-my-bills/automated-meter-reading-frequently-asked-questions.page.

025 For more on the FORT, see https://www1.nyc.gov/assets/dcas/images/fleet/video/FORT_Video_2018_112618.mp4.

026 For more on *Vision Zero*, and how the Speed Camera program vits into it, see https://www1.nyc.gov/content/vision-zero/pages/ and https://www1.nyc.gov/content/visionzero/pages/enforcement.

027 For details about the Speed Camera initiative, and the State law that expanded its reach, see https://www1.nyc.gov/html/dot/downloads/pdf/2014-10-speed-camera-faq.pdf and https://www1.nyc.gov/html/dot/html/pr2019/pr19-036.shtml.

028 For more on DOT’s Red Light Camera program, see https://www1.nyc.gov/html/dot/downloads/pdf/nyc-red-light-camera-program.pdf.

029 See, e.g., Cuba, Julianne, *“Vision Zero Cities: Removing Police from Traffic Enforcement is Crucial–and Hard!”* Streetsblog (October 21, 2020) at https://nyc.streetsblog.org/2020/10/21/vision-zero-cities-removing-police-from-traffic-enforcement-and-self-enforced-streets/.

030 For more on the *Connected Vehicle Project*, see https://www.cvp.nyc/.

031 Ibid.

032 For more on *ParkNYC*, see https://www.nyc.gov/html/dot/html/motorist/motorist.shtml and https://parknyc.parkmobile.us/parknyc/.

033 For more information about MIT’s *Senseable City Lab,* see http://senseable.mit.edu/.

034 For more on *NYC Cyber Command*, see https://www1.nyc.gov/site/cyber/about/about-nyc-cyber-command.page.

035 Figures as reported at https://www.citibikenyc.com/about. Since the beginning of the COVID-19 pandemic, CitiBike has provided free annual memberships to essential workers with nearly 850,000+ trips taken by 19,200+ members since March 2020.

036 For more on this pilot, see https://www1.nyc.gov/html/dot/html/pr2018/pr18-039.shtml.

037 In 2021, NYC DOT will launch a new dockless bicycle sharing pilot on Staten Island in partnership with Beryl, a United Kingdom-based bike share company. Beryl will launch with 350 bikes and 160 designated Beryl bike parking corrals, known as Beryl Bays.

038 For the text of *Local Laws 47* and *50*, see https://nycdotcarshare.info/sites/default/files/2017-08/Local%20Law%2047%20of%202017_0.pdf and https://nycdotcarshare.info/sites/default/files/2017-08/Local%20Law%2050%20of%202017_0.pdf, respectively. For more on the carshare pilot, see https://nycdotcarshare.info/.

039 As Revel has operated and expanded its services, it has engaged in regular communications and voluntary coordination with NYC DOT.

040 See, e.g., Kuntzman, Gersh, *"Revel Scooters Quietly Creates New Manhattan Service Area, Plus Free Use for Health Workers,"* Streetsblog, (March 26, 2020).

041 In response to a sudden spate of fatal crashes involving Revel mopeds in mid-2020, following a period of rapid growth, Revel briefly suspended service in July 2020. Revel and NYC DOT reached an interim agreement, which included new safety, user training, and accountability protocols, and the company restarted operations in late August. Moving forward, the City plans to adopt formal rules to govern shared moped systems, such as Revel. See the NYC DOT's press release at https://www1.nyc.gov/html/dot/html/pr2020/pr20-035.shtml.

042 To view the *Request for Expressions of Interest* for this pilot program, see https://www1.nyc.gov/html/dot/downloads/pdf/rfei-scooter-pilot-2020.pdf.

043 Buildings contribute 71% of total citywide greenhouse gas emissions. For more on this, and the Climate Mobilization Act, see: https://council.nyc.gov/data/green/, and https://www1.nyc.gov/site/sustainability/legislation/climate-mobilization-act-2019.page

044 For more on *Perceptive Things*, see https://www.perceptivethings.com/
For more on *Radiator Labs*, see https://www.radiatorlabs.com/.

045 See, e.g., Gensler, *"How can we integrated IoT sensing into a mixed-methods approach,"* (2018) at https://www.gensler.com/research-insight/gensler-research-institute/using-iot-technology-to-drive-evidence-based-design, and Lau, Wanda *"WeWork takes on Design Research and the Internet of Things,"* Architect Magazine (August 18, 2016), at https://www.architectmagazine.com/technology/wework-takes-on-design-research-and-the-internet-of-things_o

046 For information about the *Urbantech NYC* program, see https://edc.nyc/program/urban-technology-nyc.

047 For more about *New Lab*, see https://newlab.com/;
for more about *Company*, see https://company.co/.

048 For more on the *Neighborhood Challenge: Tech Forward* program, see https://edc.nyc/press-release/nyc-relaunches-neighborhood-challenge-tech-forward.

049 For more on *Futureworks NYC*, see https://futureworks.nyc/.

050 For more on this project, and the broader *Brownsville NYC[x] Co-Lab*, see https://www1.nyc.gov/assets/cto/#/project/brownsville-co-lab.

For more on the *NYC[x] Co-Lab* in Inwood & Washington Heights, see https://www1.nyc.gov/assets/cto/#/project/inwood-co-lab.

051 See https://www.cosmos-lab.org/.

052 The text of *Local Law 245* can be found at https://www1.nyc.gov/assets/moip/downloads/pdf/Local_Law_245.pdf.

053 The text of *Executive Order 34* can be found at https://www1.nyc.gov/assets/home/downloads/pdf/executive-orders/2018/eo-34.pdf.

054 For more on MOIP's work, see https://www1.nyc.gov/site/moip/index.page; the text of the *Citywide Privacy Protection Policies and Protocols* can be found at https://www1.nyc.gov/assets/moip/downloads/pdf/citywide_privacy_protection_policies_and_protocols.pdf.
The Citywide Privacy Protection Policies and Protocols also outlines privacy principles and directs City agencies to incorporate them into *"all aspects of agency decision-making and operations where individuals' privacy interests are implicated, whether directly or indirection."* The principles include "*Accountability, Public Trust, Responsible Governance and Stewardship, Data Quality, Integrity, and Accuracy, and Security Safeguards*."

055 The text of *Local Law 222* can be found at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3700218&GUID=A6DF2849-07C4-46D1-B1DB-27C69E989808&Options=&Search=.
The City's Open Data Law can be found at https://www1.nyc.gov/site/doitt/initiatives/open-data-law.page.

056 For more on the the NYC Open Data program, including a 2019 Strategic Plan for the program, see https://www1.nyc.gov/site/analytics/initiatives/open-data.page and https://moda-nyc.github.io/next-decade-of-open-data/.
More on MODA can be found at https://www1.nyc.gov/site/analytics/index.page

057 For more on the AMPO, see: https://www1.nyc.gov/site/ampo/index.page.

058 *"Declaration of Cities Coalition for Digital Rights,"* Cities Coalition for Digital Rights (No Date) at: https://citiesfor-digitalrights.org/declaration..

059 More information on citywide digital inclusion and digital literacy programs can be found at https://www1.nyc.gov/assets/cto/#/project/digital-inclusion-initiatives.

060 For more about the SPEC, see https://seniorplanet.org/locations/new-york-city/chelsea-center/.

061 See, for example, programs available at the Queens Public Library's *Queensbridge Tech Lab*, at https://www.queenslibrary.org/programs-activities/technology-training/queensbridge-tech-lab.

062 For more on *NYC Digital Safety*, see https://nycdigitalsafety.org/.

063 The NYCDOE is working to develop a similar offering for high school students.

064 See https://www.cosmos-lab.org/cosmos-toolkit/.

065 See https://www.cosmos-lab.org/cosmos-toolkit/index.php/edu-cational-toolkit/index.html.

066 *CUNY Building Performance Lab, About Us*, at: https://www.cunybpl.org/about-us/.

067 For more on the *Building Performance Lab* and its workforce training programs, see https://www.cunybpl.org/.

068 See, for example, Iyawa, Gloria Ejehiohen, Vijayalakshmi Velusamy, and Selvakumar Palanisamy, *"Wearable Technologies for Glucose Monitoring: A Systemic Mapping Study of Publication Trends,"* The IoT and the Next Revolutions Automating the World (2019) at https://www.igi-global.com/chapter/wearable-technologies-for-glucose-monitoring/234025

069 See, e.g., Newman, Daniel, *"Return on IoT: Dealing with the IoT Skills Gap,"* Forbes (July 30, 2019) at https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/?sh=672c-da617091, and *"IoT Signals,"* Microsoft, (October, 2020) at https://azure.microsoft.com/en-us/iot/signals/#commerical.

070 Population figure is based on the 2019 U.S. Census Bureau population estimates, as presented in Department of Citywide Planning,Population Division *"Current Estimates of New York City's Population for July, 2019,"* (2019) at https://www1.nyc.gov/assets/planning/download/pdf/planning-level/nyc-population/new-population/current-populatiion-estimattes.pdf?r=2019.

071 For more on New York City's efforts to support M/WBEs, see https://www1.nyc.gov/nycbusiness/mwbe

072 The *Citywide Privacy Protection Policies and Protocols* are available at: https://www1.nyc.gov/assets/moip/downloads/pdf/citywide_privacy_protection_policies_and_protocols.pdf.

073 *Citywide Cybersecurity Program Policies and Standards* are available at: https://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page (accessed on December 4, 2020).

074 For more information, see https://trustabletech.org/.

075 See, e.g., Paul, Keri, *"Smart doorbell company Ring may be surveilling users through its app,"* The Guardian (January 29, 2020) at https://www.theguardian.com/technology/2020/jan/29/ring-smart-doorbell-company-surveillance-eff-report, or Guariglia, Matthew, *"What to Know Before You Buy or Install Your Amazon Ring Camera,"* Electronic Frontier Foundation (February 4, 2020) at https://www.eff.org/deeplinks/2020/02/what-know-you-buy-or-install-your-amazon-ring-camera.

076 Ibid.

077 See, e.g., Cox, Joseph and Samantha Cole, "How Hackers are Breaking into Ring Cameras," Vice (December 11, 2019) at https://www.vice.com/en/article/3a88k5/how-hackers-are-breaking-into-ring-cameras.

078 Buddington, Bill, *"Ring Doorbell App Packed with Third-Party Trackers,"* Electronic Frontier Foundation, (January 27, 2020), at https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers.

079 Ibid.

080 See, e.g., Molla, Rani, *"Activists are pressuring lawmakers to stop Amazon Ring's police partnerships,"* Vox (October 8, 2019) at https://www.vox.com/recode/2019/10/8/20903536/amazon-ring-doorbell-civil-rights-police-partnerships, or Kelley, Jason and Matthew Guariglia, *"Amazon Ring Must End Its Dangerous Partnerships With Police,"* Electronic Frontier Foundation (June 10, 2020) at https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police.

081 See, e.g., Finch, Michael, II, *"California Police, Amazon Ring Partnerships Raise Concerns,"* GovTech (July 6, 2020) at https://www.govtech.com/public-safety/California-Police-Amazon-Ring-Partnerships-Raise-Concerns.html. Note that the New York Police Department does not currently have a partnership with Ring.

082 See, e.g., Guariglia, Matthew, and Bill Budington, *"Ring Updates Device Security and Privacy-But Ignores Larger Concerns,"* Electronic Frontier Foundation (February 18, 2020) at https://www.eff.org/deeplinks/2020/02/ring-updates-device-security-and-privacy-ignores-larger-concerns.

083 Ibid.

084 See, for example, Newman, Jared, *"Amazon's Ring Will Let Users Opt Out of Sharing Data with Other Companies,"* Fast Company (February 14, 2020) at https://www.fastcompany.com/90464883/amazons-ring-will-let-users-opt-out-of-sharing-data-with-other-companies.

085 Haily, Ruth, *"Fitbits and other wearables may not accurately track heart rates in people of color,"* Stat (July 24, 2019) at https://www.statnews.com/2019/07/24/fitbit-accuracy-dark-skin/.

086 See, e.g., Eubanks, Virginia "*Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor"*, St. Martin's Press, New York (2017), or Bedoya, Alvaro, *"The Color of Surveillance: What an infamous abuse of power teachers us about the modern spy era,"* in Slate (January 18, 2016) at https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.

087 For more on this effort, see https://betterbikeshare.org/wp-content/uploads/2017/06/Restoration-NACTO_BikeShareEquity_Report_WEB_FINAL.pdf. More on the broader *Better Bike Share* organization can be found at https://betterbikeshare.org/. There is more information on *Citi Bike* later in this section.

088 *"Array of Things,"* Array of Things, the University of Chicago (2020) at https://arrayofthings.github.io/

089 City of Chicago, *"Array of Things Operating Policies,"* City of Chicago (August 15, 2016) at http://arrayofthings.github.io/final-policies.html.

090 The City of Chicago Data Portal is available at https://data.cityofchicago.org/.

091 STEAM is an acronym for *"Science, Technology, Engineering, Arts and Mathematics."*

092 *LoRaWAN* is a long-range, low-power communications protocol used for IoT applications. For more information about *The Things Network*, see: https://www.thethingsnetwork.org/.

093 The team's website can be found at https://remteam28.wixsite.com/website.

094 Lexus Newsroom, *"Green for Going Green –Winning Students Tackle Global Environmental Issues in 2020 Lexus Eco Challenge,"* (April 16, 2020) at https://pressroom.lexus.com/green-for-going-green-winning-students-tackle-global-environmental-issues-in-2020-lexus-eco-challenge/.

095 For more on *COVIDsafe*, see https://www.health.gov.au/resources/apps-and-tools/covidsafe-app;
for more on *TraceTogether*, see https://www.tracetogether.gov.sg/;
for more on the *SafeEntry* program, see Tham, Irene, *"TraceTogether App's Upgrade Will Contact Tracing Smoother for Tourists,"* Straits Times (November 15, 2020) at https://www.straitstimes.com/singapore/upgrade-to-contact-tracing-app-will-make-it-smoother-for-tourists.

096 For more on the token component of this project, see https://www.tracetogether.gov.sg/common/token/.

097 See, e.g., Bostock, Bill, *"South Korea launched wristbands for those breaking quarantine because people were leaving their phones at home to trick government tracking apps,"* Business Insider (April 11, 2020) at https://www.businessinsider.com/south-korea-wristbands-coronavirus-catch-people-dodging-tracking-app-2020-4

098 For more on the *COVID Alert NY* app, see https://coronavirus.health.ny.gov/covid-alert-ny.

099 For more on this effort, see https://covid19.apple.com/contacttracing

100 See, e.g., Deffenbaugh, Ryan, *"NY Covid Alert App Exceeds 500,000 Downloads,"* Crains New York, (October 21, 2020) at https://www.crainsnewyork.com/technology/ny-covid-alert-app-exceeds-500000-downloads.

101 For more on this project, see https://www.mta.info/press-release/nyc-transit/mta-announces-new-real-time-bus-ridership-tracker-web-and-app-0

102 For more on the *LIRR TrainTime* app, see https://app.mylirr.org/.

103 For more on this effort, see https://www.mta.info/press-release/metro-north/mta-unveils-new-capacity-tracking-and-real-time-location-features-metro.

104 For more on the *Taipei Metro* measures, see https://english.gov.taipei/covid19/News_Content.px?n=D22A801689E62181&sms=DFD7BFAE73CC0B5C&s=7B0DB97F08EA0C12.

105 For more on *Kando*, see https://www.kando.eco/.

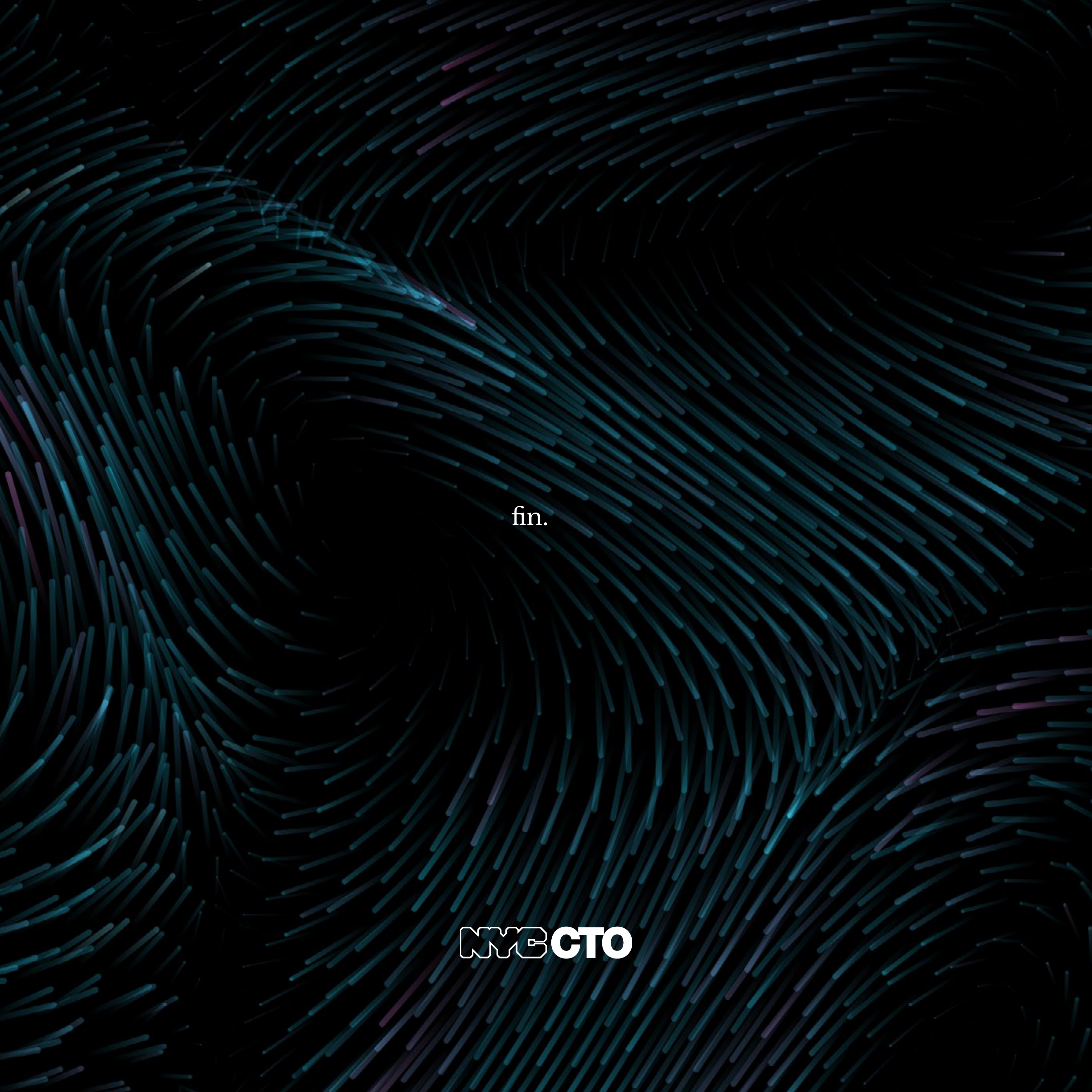
106 Pickman, Ben, *"The Story Behind the Ring that is Key to the NBA's Restart,"* Sports Illustrated (July 1, 2020) at https://www.si.com/nba/2020/07/01/oura-ring-nba-restart-orlando-coronavirus.

[107] McGee, Patrick. "*COVID-detecting 'smart rings' to be trialed by staff at Las Vegas resort,*" Financial Times (June 16, 2020) at https://www.ft.com/content/e3ab6110-b871-4cb4-abec-b195c0a88a9c.

[108] See, e.g., Xiao, Eva, "*Covid-19 Raises Demand for Temperature Scanners,*" The Wall Street Journal (May 21, 2020) at https://www.wsj.com/articles/coronavirus-raises-fever-for-infrared-skin-temperature-scanners-11590066006

[109] See, e.g., Hornyak, Tim, "*What America can learn from China's use of robots and telemedicine to combat the coronavirus,*" CNBC.com (March 18, 2020) at https://www.cnbc.com/2020/03/18/how-china-is-using-robots-and-telemedicine-to-combat-the-coronavirus.html

List of Figures



fin.

NYC CTO