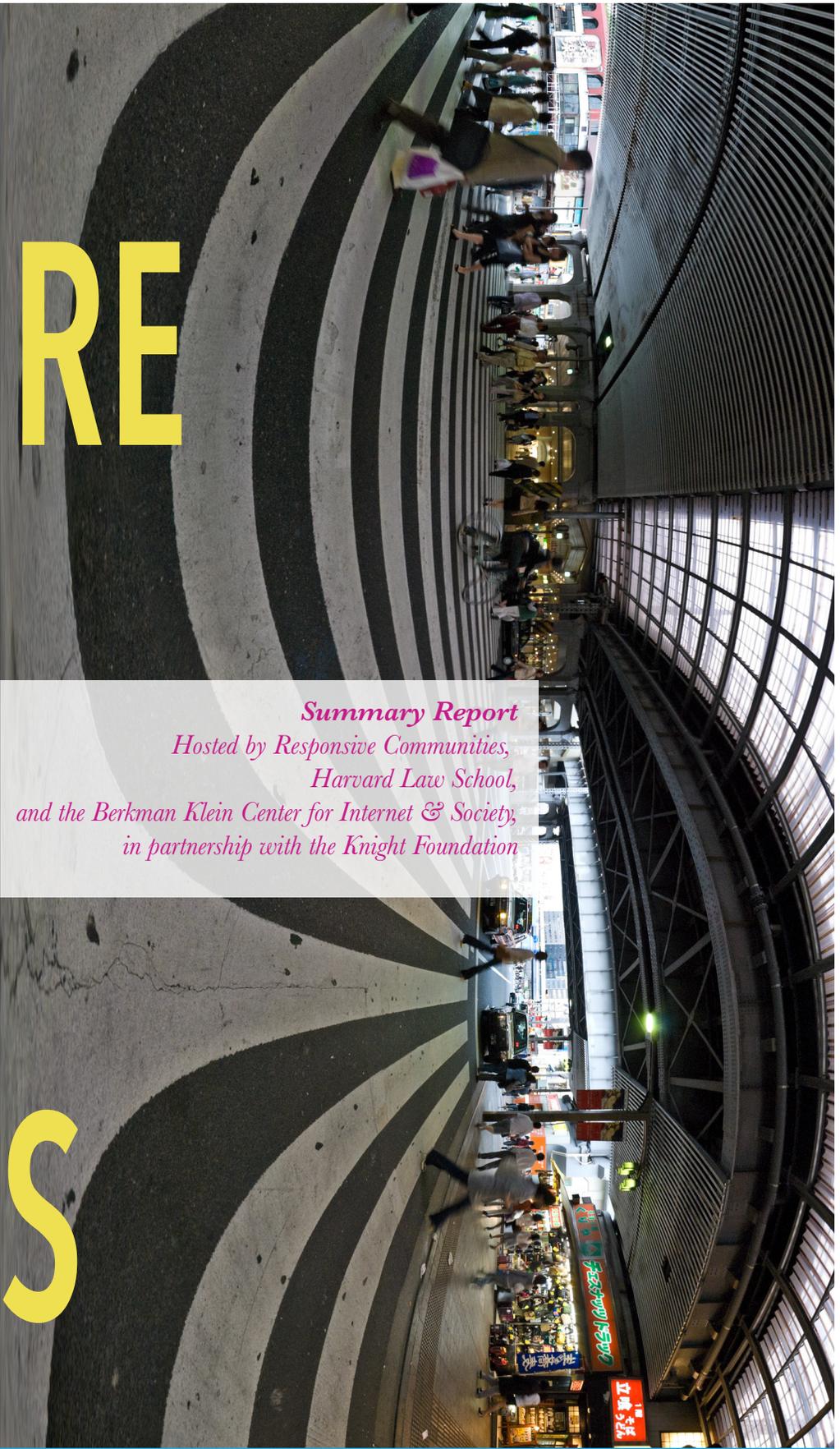


the
FUTURE
of
IoT
in
CITIES



Summary Report
Hosted by Responsive Communities,
Harvard Law School,
and the Berkman Klein Center for Internet & Society,
in partnership with the Knight Foundation



THE FUTURE OF IoT IN CITIES

Summary Report

Hosted by Responsive Communities, Harvard Law School, and the Berkman Klein Center for Internet & Society, in partnership with the Knight Foundation

Release date: April 10, 2017

The Internet of Things (IoT) is the current fascination of the technology sector. Rapid increases in computing power and the diminishing cost of sensors have produced a data gold rush as firms compete to create new data sources and new uses for that data. Cities will play a central role in this arena: while IoT is pursued across sectors, many of the use cases involve gathering data from public spaces and using these to inform municipal systems ranging from transportation and parking to water and energy management.

On November 4, 2016, Responsive Communities, an initiative of Harvard Law School and the Berkman Klein Center for Internet & Society, convened 17 city officials from across the US and abroad, along with non-profit, philanthropic, and research representatives, to discuss the future of IoT in cities. The conversation was organized around three issues: learning from early implementations, building public trust, and monetizing technology assets. The convening used these concepts, derived from preliminary interviews, to structure the conversation. From these starting points, participants shared their experiences and expert insight.

The discussion was immensely fruitful, revealing new connections across the organizational, ethical, and technical challenges presented by IoT and potential opportunities for improving public services and financial sustainability. This document summarizes insights clustered around five key themes as they emerged from the discussion: managing partnerships and vendor relations; developing the public workforce; ensuring governance and interoperability; prioritizing the public good; and expanding public engagement. After reviewing the rich insights that emerged across these five areas, this report concludes by summarizing directions for future action.

DISCUSSION THEMES AND FINDINGS

1. Managing partnerships and vendor relations

Cities often work with partners—including universities, nonprofits, and vendors—to implement IoT. The most important partner is often a vendor: cities are developing innovative collaborations with private sector partners, from established telecommunications companies to startups offering new analytics tools. But vendor relations also pose critical challenges for city agencies. Some of these are the common issues of vendor management: developing effective contracts, ensuring that vendors deliver on their commitments, and educating vendors as to city needs. Others are specific to IoT: in a contract with a vendor, who owns the data? What level of privacy needs to be enforced, and what monetization schemes are acceptable?

a. Vendor training

Each city has specific service and policy missions and vendors' products are not always a perfect fit. As one official explained, when it comes to IoT, "We're often finding that there's a gap, sometimes quite a large gap, between the way that vendors approach us and the kinds of challenges that we want to take on." Several attendees conveyed their sense of being overrun with vendor requests before their cities had decided what their own goals were for IoT systems.

To maximize the value of vendor relationships, some cities have started to engage in vendor education. Cities bring firms into their agencies to provide insight into specific needs and determine whether those needs can be addressed with an existing solution or through the development of a new product. This kind of education can shift the relationship between vendors and cities from sales to collaboration, and can enrich vendors' offerings. When extensive collaboration leads to a new solution, cities may be able to contract for joint licensing rights when vendors offer these tools to other cities: Cities "buy solutions from other companies all the time so why can't [we] be a partner in the development and benefit from the revenue?"

Vendor education can lead to productive collaboration, but cities are also learning to say "no" when vendor solutions do not align with city needs. As one official put it: you have to ask, "Can it help me achieve the goals that [we] have as a city?" If yes, cool, let's implement it. If not, well, no thanks... [Our city is] big on saying, "Well, if it doesn't help us in getting a more livable city, if it doesn't help us [move] forward, then why should we accept a new solution that may... actually encroach on our privacy?" The answer is often, no.

b. Coordination and reducing redundancies

City agencies often lack clear channels of communication, creating redundancies in vendor contracts. While it is important for agencies to have flexibility, centralized decision-making helps to identify common needs and safeguard against excessive customization, increasing the chances that cities can leverage technologies across multiple agencies.

Cities are beginning to experiment with centralized technology planning and purchasing, allowing them to identify opportunities for inter-agency collaboration, discover new synergies, and prevent redundant technology investments. As one official explained, “We do have budget centralization. I do have the authority to cancel or deny any spend across any agency if I don't think it's in the right interest of the city.”

Such centralized decision-making can ultimately reduce costs. While central decision-makers put citywide efficiency and effectiveness first, agencies often get mired in customization: “When you look at certain enterprise application rollouts in other agencies, the costs are significant because, usually, it's a functional person making a decision about the system, so they end up spending way more” on development, operations, and maintenance.

c. Data and infrastructure ownership

Vendor education and centralized decision-making are issues across all types of vendor relationships, but IoT presents new challenges specific to data and infrastructure. IoT programs rely on three “layers”: (1) physical infrastructure, including sensors, fiber networks, and data storage; (2) data collection, aggregation, and management systems; and (3) the applications and services that use data to serve government workers and the public. Vendors offer products and services at all three levels.

In engaging with vendors, cities must consider who will own the product, the layers on which the product operates, and the implications it may have for other layers. If one vendor provides the physical infrastructure, they may also have access to data—does that raise concerns? If a vendor offers data collection and management as a service, will the vendor own the data or will the city? Are there circumstances in which the city risks losing either access to data or control over mechanisms such as privacy restrictions?

In some cases, cities are finding that they risk ceding control over their own data and will be forced to pay for access to that data, often indefinitely. Cities are thinking strategically about each of these layers and their interdependencies, but there are many complex factors at play and each solution must be negotiated individually.

d. Establishing privacy ground rules

While each IoT solution will trigger its own concerns, some cities are starting to establish universal ground rules for privacy. Through the enactment of agency policies or legislation, cities can decide that certain commitments are required of any vendor. If the vendor does not agree to ensure the established level of data privacy, the city will simply not work with them. Such universal ground rules can be highly effective for demonstrating the city's commitment to privacy, both to the public and to vendors.

It is particularly important to establish specific and concrete privacy expectations when working with vendors. When cities rely on vendors' technology, it is the vendors that create the privacy ecosystem. If privacy protections are not negotiated and guaranteed at the outset, cities have

limited options for protecting the privacy of any data or system connected to the IoT system. Since vendors have less investment in privacy expectations, cities must drive appropriate privacy practices.

As technology continues to evolve, however, cities risk committing to principles now that will not make sense later as new capabilities become available and public opinion shifts. Many officials said it was difficult to navigate these tradeoffs: “That’s a huge wildcard for us... because the very heart of technology is that it’s constantly evolving and constantly changing. We can come up with a set of guidelines that will say, ‘We will do this, this, and this’... But that could change in a few years as technology evolves.”

In place of established policies, cities are seeking to develop “resilience frameworks” that set out certain commitments while making room for development. As one participant explained, “We need to know there are certain things that we can’t predict... We need to accept that... and know that we are taking this journey together with the utmost intention of following the overall goal. But to end up with a privacy policy that clearly defines everything and is static, and we won’t need to look at it again, I think it is actually unrealistic.”

e. Non-vendor partners

Cities also collaborate with other institutions in developing new IoT programs. Universities have been particularly important, contributing to research and development as well as providing analytic capacity. As interest grows, there is room to harness the extensive talent available through local universities to advance a city’s technology agenda. In particular, universities are often trusted actors in the community and can act as an intermediary between cities and vendors to mitigate concerns about issues like privacy and data ownership. While cities value these partnerships, they are not a replacement for vendor expertise. As one official put it: “As much as I’d love to source all of our IoT from the [local university], we’re going to buy things from Verizon, we’re going to buy things from all these companies.”

2. Workforce development

As cities expand their use of IoT, it becomes increasingly important that city agencies have the talent to manage and analyze complex data systems in-house. Innovation has always been a challenge for cities: long-term employees can be reluctant to embrace new tools and practices, while bringing in new, often young employees can produce internal cultural strains and pose difficult workforce retention issues. In order to get the best value out of IoT, cities will have to attract new talent while retaining and cultivating existing staff resources.

a. Technology change and workforce training

It is an old cliché that government workers resist innovation. While the workforce is generally more flexible and forward-looking than the public imagines, cities still struggle with entrenched practices and incentive systems that promote the protection of old technologies and resistance to new solutions. Long-time employees may see technology as a threat to their job security. To

counteract the tendency to protect the status quo, cities can guide employees in learning how IoT will help them—serving to enhance rather than replace their roles.

As one official explained, “If you think about that perspective of the twenty-year veteran, these are all programs that are attacking them.” In order to take advantage of IoT, cities must work to familiarize the workforce with new technology, train them to use it in their daily practice, demonstrate how to leverage IoT within their workflow, and cultivate a commitment to innovation. Strong workforce training programs build such capacity and engender enthusiasm among city workers. In doing so, they also build a new audience for proliferating data streams available through IoT: when city workers are data-literate, they can find new uses for available data and put it to work on behalf of the city.

b. Building employee engagement

While broad enthusiasm for technological innovation can create a forward-looking culture, cities must also work to develop employee buy-in on a project-by-project basis. The success of new IoT initiatives depends on the support of the employees who implement and maintain them. Cities are starting to find ways to build employee ownership through training and public engagement. Some cities offer a “data camp” that gives employees a crash course in the tools that IoT makes available. Others send workers to civic hackathons to see, in person, how excited citizens are about the new technologies and the effect of these programs in the field. Bringing employees into the process *early*, in setting goals and envisioning design for IoT projects, and bringing them in *often*, with updates and demos, increases the likelihood of project success and long-term returns.

c. Attracting and retaining young and highly-skilled workers

For a variety of reasons, cities have long struggled to attract and retain highly skilled employees. But a new generation of workers is leaving college with technical skills and an appetite for public service. Attendees agreed that ensuring a broad pipeline of new local government employees cross-trained in policy and technology is critical to the future success of cities.

As cities benefit from the energy and expertise of these employees, they are beginning to consider how to effectively retain them. One challenge is to build bridges between old and new employees: if the existing workforce resists change while new employees promote it, agencies can experience cultural strain and gridlock. Additionally, new employees coupled with new technology can exacerbate anxiety about job security and status among veteran employees.

The more workers can engage with others collaboratively, the more opportunities there are for older employees to learn from the technical insights of new ones and for new employees to enrich their understanding of the city through the institutional knowledge of the long-term workers. Cultivating this collaborative culture can lead to faster, more visible outcomes. These outcomes, in turn, help with retention: showing workers that their efforts make a difference in the lives of citizens is central to motivating them to continue in public service.

3. Governance and interoperability

As data increases in scale, it increases in value. To derive the greatest benefits, IoT systems must be fully integrated: a patchwork of IoT projects that cannot speak to one another will yield only a small return on investment. Ensuring interoperability is a leadership challenge. The earlier cities make it a priority, the easier it will be.

a. Inter-agency collaboration

Smart planning starts with inter-agency collaboration. Silos are a persistent challenge in government, but integration is of particular importance to IoT. Participants identified two strategies for facilitating project success. First, technology should be integrated into broader planning and policy processes. By aligning technology investments with citywide goals, officials can more clearly demonstrate a project's value. Along the way, IoT projects can be reframed not as "technology" projects but as crucial components of sustainability, mobility, or health agendas.

Second, even as IoT projects are integrated into citywide planning, they must retain technical leadership by specialists. Participants described setbacks experienced when, for example, transportation officials were tasked with leading IoT projects. Collaboration is critical but thoughtful, collaborative technology experts are needed to take on leadership roles in these inter-agency projects.

b. Standardization

Standardization is essential to the value of IoT projects and the efficiency of new project development. Participants addressed the importance of standardization at different levels, starting with the benefits of standardizing street furniture to facilitate sensor and other infrastructure installation. Building up from this infrastructure, standardized data architecture facilitates integration and data sharing across agencies, amplifying the value of data. Setting standards can also help ensure data quality, increasing the usability of data both within and beyond government. Finally, standard security controls are critical to ensuring robust protection for personal data. Standardization is thus key to the efficiency, value, and security of IoT projects—it must be a top priority as cities embrace these new tools.

At the level of government operations, standardization can also facilitate cooperation and accountability. By establishing clear, common standard for the implementation of IoT projects, cities can ensure that all agencies integrate new systems with existing infrastructure and develop internal reporting systems to enhance accountability. This procedural standardization, however, poses challenges to management operating in new territory: while IoT is still rapidly evolving, officials will need the flexibility to make rapid operational decisions. Standardized procedures should enable rather than inhibit such autonomy.

Participants highlighted the critical role of leadership in facilitating collaboration and the adoption of a common set of standards. In one city, for instance, the centralized authority of the city's Chief Operations Officer facilitated rapid alignment of standards across agencies, as the adoption of central standards became a prerequisite for accessing funds from City Hall.

c. Budgeting, collaboration, and sustainability

City officials described the negative consequences of inter-agency competition: when agencies are competing with one another for a larger slice of the budget, they can lose out on opportunities to reinforce broad city goals. Reframing technology as integral to other city goals can facilitate collaboration and allow officials to identify mutually beneficial opportunities. This integrated approach also helps to make the benefits of technology visible to citizens, who are typically more concerned with material outcomes than operational efficiencies. Bringing the benefits of technology to light can build support for further projects.

Federal funding often imposes limitations on the use of funds or the use of the funded project that artificially limits possibilities: assets funded through federal agencies create multiple uses and smart technology will both save costs and expand functionality across agencies. As discussed below, a loosening of restrictions on federal grants would allow cities to foster this inter-agency planning and bring technology into the “nerve center” of the city.

To advance a more effective funding model, city representatives should have an active role in federal-level discussions. A recent meeting of the President’s Council of Advisors on Science and Technology, which focused on cities, involved only nominal city representation. But cities should be at the heart of the process shaping federal technology policy, both urban and national.

Participants also addressed the persistent problem of sustainable funding for technology projects. Cities often receive funds for capital investments without commitments to support operational expenses. Like other forms of infrastructure, there is potential to build refreshment or replacement commitments into city proposals. Where such funds are not available, infrastructure and data monetization can provide revenue to support maintenance, operations, and upgrading.

d. Scaling up

Some cities have implemented successful IoT testbeds, but many still struggle to scale up. Scaling presents a number of technical and policy challenges. Cities must have extensive fiber networks available to support citywide IoT. Reaching underserved neighborhoods can be particularly challenging, which raises issues of social equity. In some cases, scaling has been facilitated by monetization: leasing infrastructure or data access to private companies can create a revenue stream to fund continued expansion and enhancements.

Participants also pointed to the potential for scaling solutions beyond city limits. In some places, multiple contiguous municipalities mean that officials have to find ways to collaborate across jurisdictions. Others pointed to the responsibility that larger cities have to serve as research and development centers for other localities, including smaller cities, towns, and counties in the region: big cities have the resources to apply for and manage grants and to implement innovative projects. They can benefit their regions by making their solutions and lessons learned available to nearby jurisdictions with fewer resources.

4. Pursuing the public good

Cities are responsible for protecting the public good. IoT presents an immense opportunity, but cities will have a critical role in directing the development of this field to maximize benefits for the public and protect the public from predatory abuses. By defining and prioritizing the public values at stake in connection with IoT, cities can guide the development of infrastructure, data, and analytics at the city level in accordance with the public good.

a. Values-driven IoT strategy

Why invest in IoT? Participants highlighted the fact that technology is not an end in itself—it is a means of achieving the city’s goals. Identifying the city’s priorities provides essential guidance for city agencies: as one official put it, “In [our city], it’s about two things: increasing livability and increasing sustainability.” Once widely known and broadly supported, such goals can serve an important coordinating function, helping officials select projects and make effective decisions throughout the development process. IoT has the potential to reduce energy consumption, improve mobility, facilitate new business opportunities, and reduce social inequality, but only if these projects are undertaken with value-based goals in view.

For many cities, the default justification for technology investments is reducing costs. But participants highlighted that such economic cost-reduction often leads to hidden costs down the line: “If you show up at our doorstep and say, ‘This will save you a bunch of money,’ somewhere along the lines we have to figure out what is the actual social and community level impact.” In some cases, cost reduction comes at the expense of data ownership and privacy protection, or of community engagement and input. Cities are learning to think ahead to the potential future impacts of technology decisions made today.

Most importantly, cities must ensure that citizens remain the top priority. Many IoT vendors view government employees as the customers, aiming to make their lives easier. But while employees may most directly use these new technologies, the customers are always the resident—a tool to improve internal workflow is only as useful as the impact it has on the lives of residents.

b. Monetization and its risks

Monetizing infrastructure and data can provide much-needed revenue to cities: cities turn their infrastructure into revenue by leasing it to firms and sell access to data in exchange for fees or revenue sharing. While, in some places, this revenue goes into the general fund, other cities are setting up systems for ensuring that the income from technology initiatives is used to fund technology maintenance and expansion, creating an economically sustainable system.

In terms of infrastructure, cities have systems for leasing access to street furniture for firms that want to set up sensors or cables and for leasing access to city fiber networks. Permission to use city infrastructure has long been a critical source of revenue. Leasing a municipal fiber network can be an extraordinarily effective way to foster competition and undermine the monopolies of the major providers. Similarly, requiring advanced wireless and IoT systems to share streetlights

and other city assets on a neutral, nondiscriminatory basis subject to reasonable fees can both provide revenue and retain the city's control over its IoT destiny.

On the data side, some cities have developed civic data exchanges, where firms can purchase access to high-quality data to inform their business practices. Cities are exploring the possibility of releasing high-quality public data on such data exchanges and offering lower-quality data on open data platforms. Making city data marketable would require improving data quality and delivery—organizations that pay for access expect reliable, real-time data. Another monetization method could feature revenue-sharing agreements with vendors for new IoT projects that sell data to advertisers. Still others allow the private sector to build infrastructure and capture data in exchange for giving cities access to a copy of the data. Attendees' approaches to these difficult and novel issues varied widely.

The monetization of personal data raises critical issues about ethics, privacy, and security. What kind of information can be collected? How will it be secured? To what extent can residents opt-out, and how do you tell them that this is an option? Cities are weighing the potential for much-needed revenue—particularly to fund the construction of IoT technologies—against concerns about putting residents' data at risk. To date, most cities are erring on the conservative side, trying to retain ownership of data, limit the collection of personally identifiable information, and leveraging data for the public good instead of making it available for sale on the market.

c. Ensuring privacy and security

Privacy and security are top concerns for city officials. As one official explained: “We are generally responsible for the safety and well-being [of] our citizens. In this realm of IoT and big data, I don't know why that wouldn't extend to the data health for our residents.” To that end, officials focus not only on ensuring the privacy and security of the data collected by the city but also on protecting citizens from private sector IoT projects that might not be in a citizen's best interest. For city projects, officials have a number of strategies for ensuring citizens are informed of developments: they focus on making privacy policies easily accessible and understandable to non-experts; they start slowly, with limited data collection; they take time to explain these new projects to citizens; and they prioritize clarity and honesty with residents about what kind of data is and is not being collected.

Some participants expressed concern that cities will inevitably cede control over privacy when they collaborate with vendors. Without strong and frequently-enforced contracts in place, vendors may find ways to exploit data that violate a city's privacy commitments. Privacy principles, discussed above, can be an important first step in signaling to vendors that cities have strong requirements when it comes to citizens' privacy rights. Some participants suggested there might be tradeoffs between privacy and monetization: citizens are more likely to share their data for the purposes of improving city services than if it will be handed off to a third-party. One participant explained: “What we have constantly communicated is that... we are not monetizing. We are collecting data to improve services for the residents... I think it's important to make that distinction.”

The flip side of strong privacy protections, however, is rigidity. When cities make strong and unqualified statements about privacy, they lose the opportunity to revise these commitments over time, as technology, financing, and public opinion change. Participants emphasized the tradeoff between building trust through the use of clear, specific, and unambiguous policies, and the ability to accommodate evolving technology.

d. Social equity as a priority

Cities are homes for diverse populations and inequality is an acute concern for public officials. Technology should be used to reduce, not to sharpen, these inequalities. Participants pointed out potential risks of IoT for disadvantaged communities. Often, residents in poor neighborhoods are more likely to welcome surveillance, out of concern for safety. But more putting more sensors in these areas—like greater police presence—can reinforce the stereotype that these neighborhoods are “problematic.” Additionally, systems that allow residents to opt out of data collection are more likely to be used by people from more privileged backgrounds. To ensure social equity, officials need to make a concerted effort to think first about the people with the fewest advantages. For these populations, in-person education and training programs can be particularly important.

5. Expanding Public Engagement: Building from the Bottom-up

As urban IoT grows, city officials must bring the public along. This involves extensive education: most citizens do not know about cities’ technological capacity, what data they collect, and what they do with the data. Engagement begins by explaining both the systems and their purpose. These efforts can be the foundation for public trust, which could enable further city projects. Engagement can also become the foundation for designing future projects: letting users decide what they need and how they prefer to get it will yield the highest quality products and the highest return on investment.

a. Citizen education: What does the city do and why?

Participants emphasized that citizens need to have a better understanding of what the city does technologically, what the options are, and where the city plans to go from here. Reaching citizens is a long-standing problem for city government, but new tools are making it easier. One official explained her city’s shift from strategy documents to videos: few people read strategy documents, while short video presentations of the city’s plans can easily reach citizens online. In addition to informing citizens of what the city *plans* to do, officials also stressed the need to show what the city has *already* accomplished. This is best achieved by showing, rather than telling: “We can talk about technology all we want. Until people can see it, they don't care about it.” Once residents understand what the city has accomplished and the plans for moving forward, they are equipped to engage in the planning process and provide valuable feedback.

b. Creating trust: Engaging openly and meeting citizens where they are

Particularly as cities move into the world of IoT, creating public trust is of paramount importance. For the city to learn from its data, citizens must be willing to share their data with the city, and citizens will not be willing to share if they do not understand and trust the city's intentions. As one participant explained: "What happens when the community doesn't understand what's happening? They go to their council member, and we tend to get our project shut down very quickly."

In order to educate citizens, participants emphasized the need to recognize that there are different populations that need to be approached differently. Young and tech-savvy citizens are eager to engage and easy to reach through social media; others lack access to these tools or familiarity with the public engagement process; and activist groups are prone to attacking the city in the press if they are not engaged in ongoing conversations.

Cities are learning to reach these populations where they are—going to the people instead of waiting for the people to come to the city. Online and through meetings, officials can engage with citizens and help them understand what technology and data mean for their lives. As one official explained, we often think about the "smart city" in terms of optimizing and efficiency, but some of the most important dimensions of technology projects focus on creating trust through person-to-person interactions. This does not look efficient in the short run, but it is critical to long-term success.

In addition to describing plans for new technologies and the benefits they will offer to citizens, it can be helpful to be up-front about what the city plans *not to do*: what data will *not* be collected and how data will *not* be used. Officials can often anticipate the public's main concerns, and, in most cases, the planned changes will not affect any of those issues. As discussed above, however, city officials have to navigate the tradeoff between being very clear and specific about the use of data and allowing room for data projects to evolve over time. Clarity and specificity help to foster public trust, but this effort is wasted if these clear boundaries are then transgressed.

c. Let the users be the guide: Employing design-based thinking

As in any design process, IoT projects benefit from the input of end-users early and often. Participants emphasized the value of user input in driving IoT plans: rather than deciding what the government wants or letting vendor solutions drive IoT deployment, officials are looking to citizens to find out what kind of data initiatives would benefit them: "You need to *ask*, first and foremost. You can't assume. Go out and ask your residents and build your projects in the context of what your residents tell you because no one else can speak for them." Just as projects should be driven initially by public input, the city should check in regularly with the community to receive feedback throughout development. Cities have used different methods to facilitate continuous engagement, including community oversight boards and monthly public meetings. Whatever format the city chooses, consistent and responsive engagement with citizens is crucial to implementing successful solutions.

MOVING FORWARD

What do cities need in order to move IoT forward quickly, effectively, and wisely? The day's discussion yielded ideas for concrete forms of support for cities from foundations, researchers, and their fellow government officials.

1. Continuing the Conversation: Participants expressed a desire to continue and expand the conversation. Cities are one another's best resource, and continued engagement opens up space for mutual learning and collaboration. Existing networks of CIOs and other city technology officials charged with making difficult values-based decisions about the future of IoT should be supported with additional philanthropic resources, supporting skilled technical/financial/policy advice to these networks. Moving forward, other stakeholders could also be brought in to enrich the conversation, including state and federal officials and citizen groups.

2. Additional Projects: Participants highlighted several additional priorities for support.

- a. **From testbeds to scale-up:** Cities have found it relatively easy to obtain funding for pilot projects, but the real benefits of this technology accrue only at scale. All cities could learn important lessons from just a few that successfully scaled IoT operations. At this stage in the development of these technologies, concentrated funding in a few jurisdictions could yield dramatic, and widespread, returns.
- a. **Measuring economic outcomes:** To make the case for IoT, cities have expressed a need for documented savings or economic returns stemming from technology investment. Evidence from past projects within the city or similar projects in other localities is essential to justifying investments in projects that are often novel to budget officials. Researchers and foundations can play a role by developing case studies that demonstrate the financial benefits of IoT.
- b. **Reducing federal grant restrictions:** Federal funding is critical to cities, but restrictions on both the use of funds and the use of the final products often narrow cities' ability to deploy this funding effectively. For instance, many US Department of Transportation grants can be used to fund only traditional transportation infrastructure, rather than sensors that will enhance that traditional infrastructure's functionality. Other grants will allow technology to be built, but *exclusively* for a specific purpose, such that cities lose the opportunity to leverage these resources for complementary purposes. Advocates can help cities progress by campaigning to reduce unnecessary restrictions on the use of federal funds.

3. Model Documents: Participants expressed a desire to access policy, contract, and business models.

- a. **Business models:** What are the business models available for IoT? What are their respective strengths and weaknesses? Cities expressed an interest in having access to a typology of IoT business models so as to inform their decision-making.
- b. **Model contracts:** Ensuring long-term city control over data and privacy is a central concern, particularly in projects involving vendors. Model contracts could facilitate more effective negotiations and help ensure that cities are protecting citizens' interests.
- c. **Model policies:** Privacy is a critical concern for all cities. But the issue is both technically and conceptually complex. Not all cities have the resources to develop effective citywide policies and most cities continue to struggle with the degree of specificity or flexibility to build into these policies. Model policy documents would help cities clarify their commitments and enforce consistent protections in contracting with vendors.
- d. **Asset valuation:** Cities have important physical and data assets, whose monetization has the potential to fund further technology investments and much-needed maintenance. But cities often do not know the value of their own assets. Guidelines that help cities value their assets will help cities maximize the returns on leasing or data-sharing agreements.

4. Evidence: Cities expressed an interest in forms of evidence that would help them make the case—to leadership and to citizens—for investing in IoT.

- b. **Citywide outcomes grounded in data:** The simplest type of evidence is outcomes from other localities. Researchers and foundations can support cities by developing detailed case studies with clear data on policy outcomes across social, environmental, and other indicators.
- a. **Lessons learned and best practices:** Cities can learn from each other. Those on the cutting edge can support less sophisticated cities by documenting outcomes and lessons learned from early IoT implementation. Researchers and foundations can further amplify the benefits of these insights by evaluating multiple cases and documenting best practices.
- b. **Quick wins locally:** Sometimes evidence from another locality is not sufficient and officials need to demonstrate the value of IoT locally. If some IoT projects are lightweight, low-cost, and yield straightforward and easily measurable benefits, these should be documented as “model projects” and made available to officials who are struggling to make the case.
- c. **Audits:** As we move into an era of machine learning and artificial intelligence, some public advocates are concerned about the capacity for these systems to reproduce or

entrench existing inequality. Experts can support cities in their pursuit of social equity by conducting and documenting audits of these automated systems and their outcomes for diverse populations.

5. Educational Tools: Cities are responsible for managing input from diverse stakeholders—including vendors, employees, and the public—in the development of IoT projects. Education is essential to ensure that vendors understand city needs and limitations; that employees will embrace and effectively manage new tools; and that the public is aware of and supports technological innovation.

Researchers, foundations, and advocates can support cities by developing educational materials and workshops on subjects for public digital literacy, city employee professional development, and vendor training. Education initiatives can increase coordination among government workers and their vendor partners and enhance the impact of IoT initiatives by educating citizens in the use of these new tools. Finally, public education programs can mitigate the inequalities that technology might otherwise create or reinforce.

6. Repository: There is a large and growing body of writing about IoT—some very useful and some simply speculative. As researchers, advocates, and foundations develop these case studies, model documents, reports, and educational tools, cities would benefit from a centralized repository. Once established, officials could be confident that information from this source is reliable and vetted by experts.

List of Attendees

Hosts

Susan Crawford, Moderator, *John A. Reilly Clinical Professor of Law, Harvard Law School*

Waide Warner, *Lecturer on Law, Harvard Law School*

Maria Smith, *Project Coordinator, Berkman Klein Center for Internet & Society*

Ben Green, *Fellow, Berkman Klein Center for Internet & Society, Data Analytics Fellow, City of Boston*

David Cruz, *Research Assistant, Berkman Klein Center for Internet & Society*

US city officials

Ted Lehr, *IT Data Architect, City of Austin*

Nigel Jacob, *Co-Chair, Mayor's Office of New Urban Mechanics, City of Boston*

Brenna Berman, *Commissioner and CIO, City of Chicago*

Forrest Toelle, *Information Technology Director, City of Columbus, Georgia*

Sam Orth, *Director of Technology, City of Columbus, Ohio*

McClain Bryant, *Director of Policy, Office of the Mayor, City of Kansas City, Missouri*

Kate Garman, *Innovation Analyst, City of Kansas City, Missouri*

Debra Lam, *Chief Innovation and Performance Officer, City of Pittsburgh*

Miguel A. Gamiño, Jr., *Chief Technology Officer, City of New York*

Will Barkis, *Volunteer Technology Advisor*, City of San Francisco
Michael Mattmiller, *Chief Technology Officer*, City of Seattle
Archana Vemulapalli, *Chief Technology Officer*, City of Washington, D.C.

International city officials

Morten Kabell, *Mayor of Technical and Environmental Affairs*, City of Copenhagen
Young-Hoon Choi, *Chief Information Officer*, City of Seoul
Amos Tan, *Director Smart Nation Solutions & Applications*, GovTech Singapore, City of Singapore
Junie Teo, *Assistant Manager (Smart Nation Solutions & Applications)*, GovTech Singapore, City of Singapore
Staffan Ingvarsson, *CEO*, AB Stokab, City of Stockholm

Non-profit and research representatives

Alaina Harkness, *Fellow*, The Brookings Institution
Cheryl Leanza, *Policy Advisor*, United Church of Christ
Joanne Hovis, *President*, CTC Technology & Energy

Foundation Representatives

John Bracken, *VP*, Technology Innovation Program, Knight Foundation
Eva Pereira, *Technology Innovation Associate*, Knight Foundation
Benji de la Peña, *Director of Community and National Strategy*, Knight Foundation
Sam Gill, *VP*, Learning and Impact, Knight Foundation
Jenny Toomey, *Director*, Internet Freedom, Ford Foundation
Michael Brennan, *Technology Program Officer*, Internet Freedom, Ford Foundation
Ryan Gerety, *Technology Fellow*, Ford Foundation
Eric Sears, *Senior Program Officer*, MacArthur Foundation