

Smart Cities & Service Improvements Committee Privacy Policy Engagement

Erica Garaffo | Data Analytics Lead, Office of Civic Innovation & Digital Strategy

Shireen Santosham | Chief Innovation Officer, Mayor's Office of Technology & Innovation

April 5, 2018

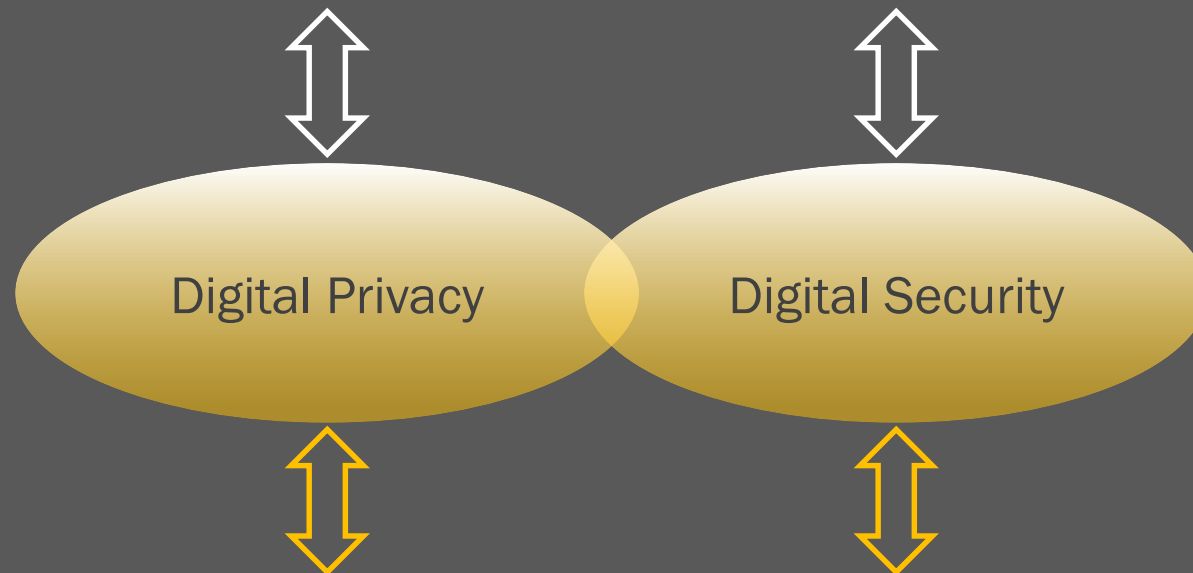
The City's current policy framework is focused on a few applications.

- The City's public-facing website
- My San Jose application
- Library's patron privacy policy

These privacy principles are point specific, but are not governed by a Citywide, overarching privacy policy.

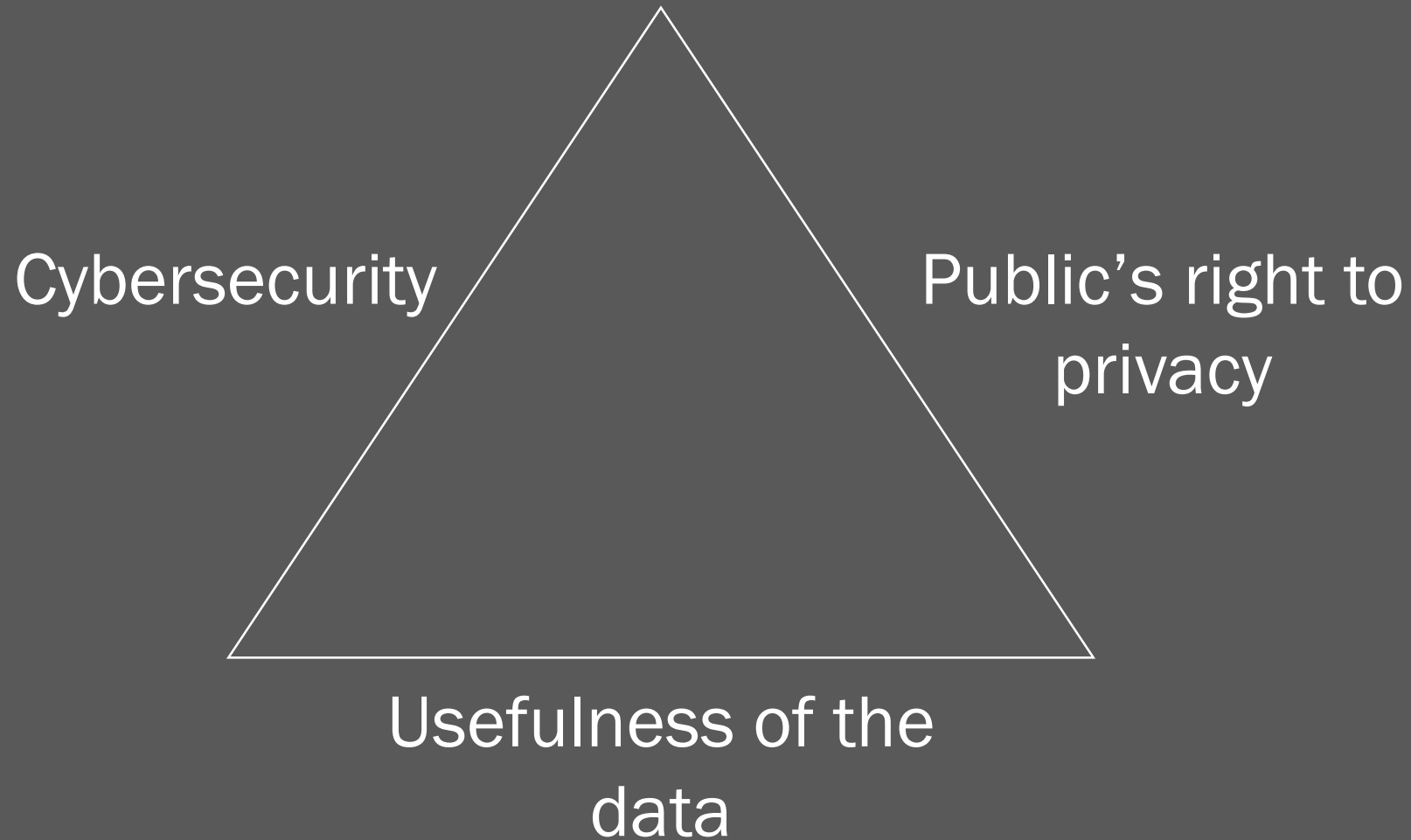
A Smart City requires a robust Privacy and Security framework.

Community, External Partners & City Stakeholder Engagement



Internet of Things – Data Collection, Use & Distribution,
Operational IT Systems & Infrastructure

We wish to strike a balance between security, privacy and utility

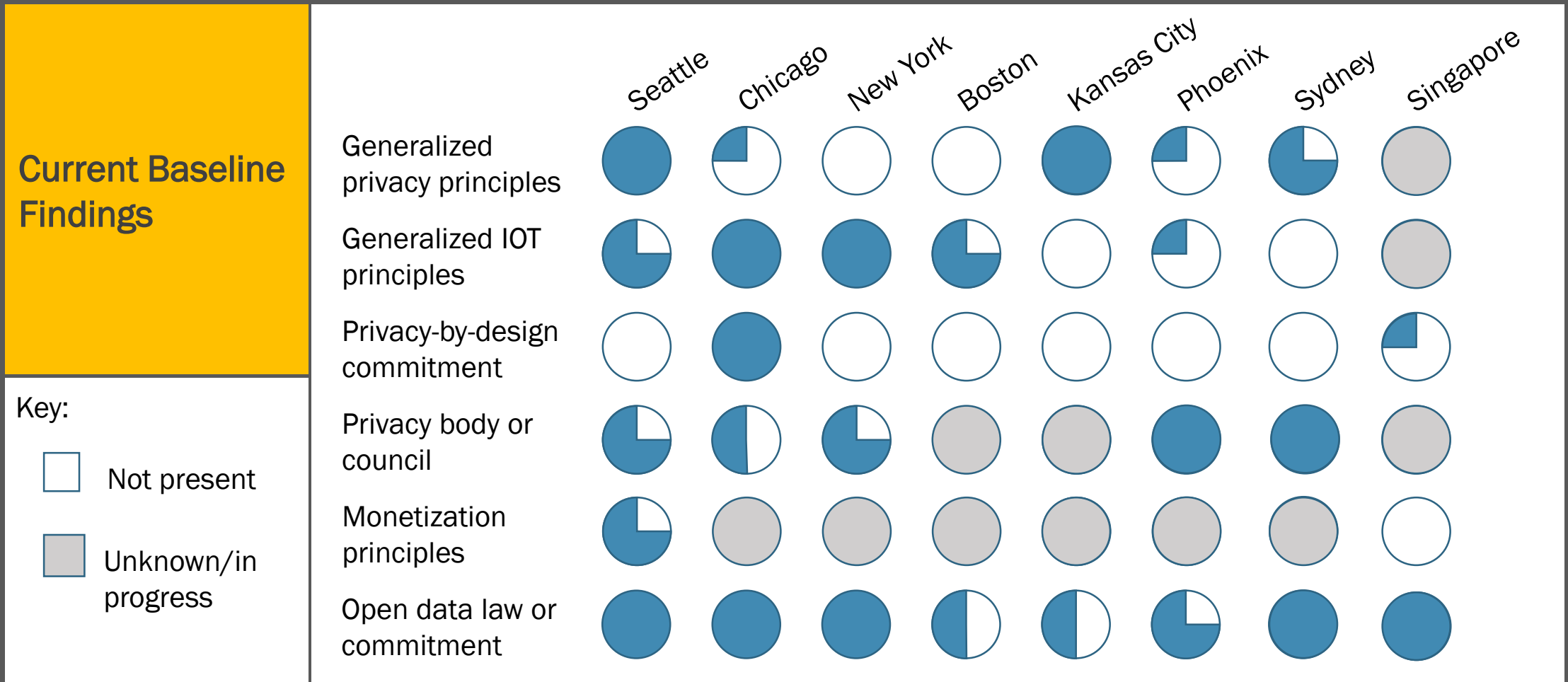


In Fall 2017, we engaged the CyberLaw Clinic at Harvard Law School

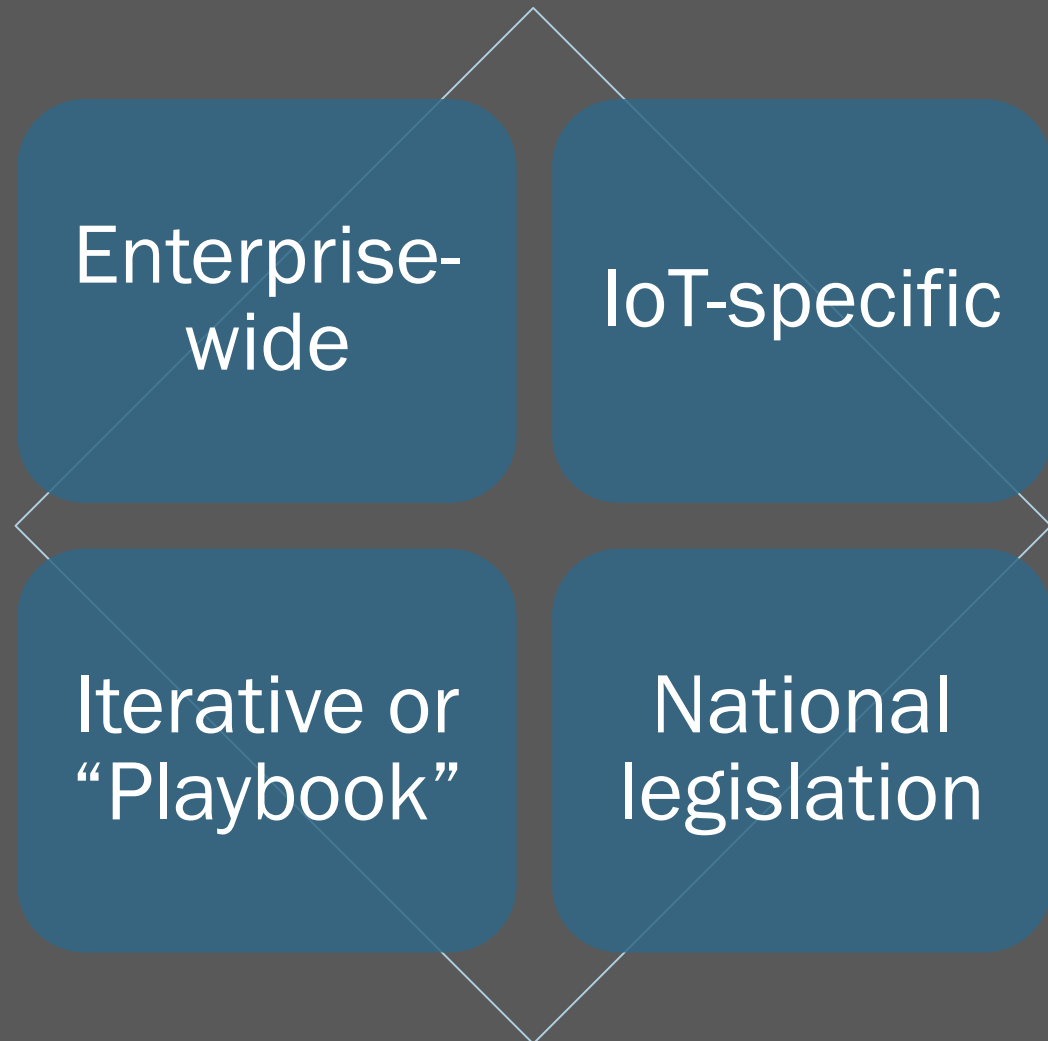
- Pro-bono legal services overseen by Professor Susan Crawford
- Mayor's office met with this group weekly
- Benchmarked 13 cities and made recommendations around San Jose's approach to privacy
 - No "one-size fits all" approach to privacy
 - Process of engagement is as important as the details of the policy
 - Single point of contact such as a Chief Privacy Officer can be helpful



Privacy approaches vary across cities and are still evolving

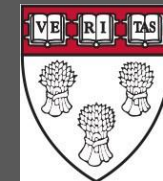
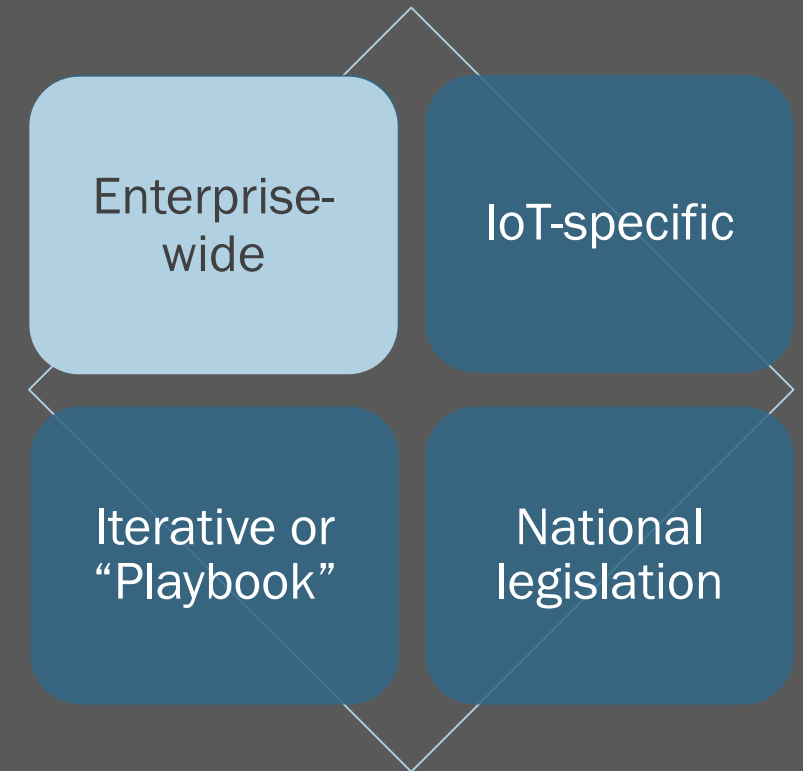


Municipal approach to privacy fits into one of four models



Enterprise-wide approach is high level.

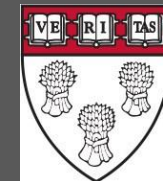
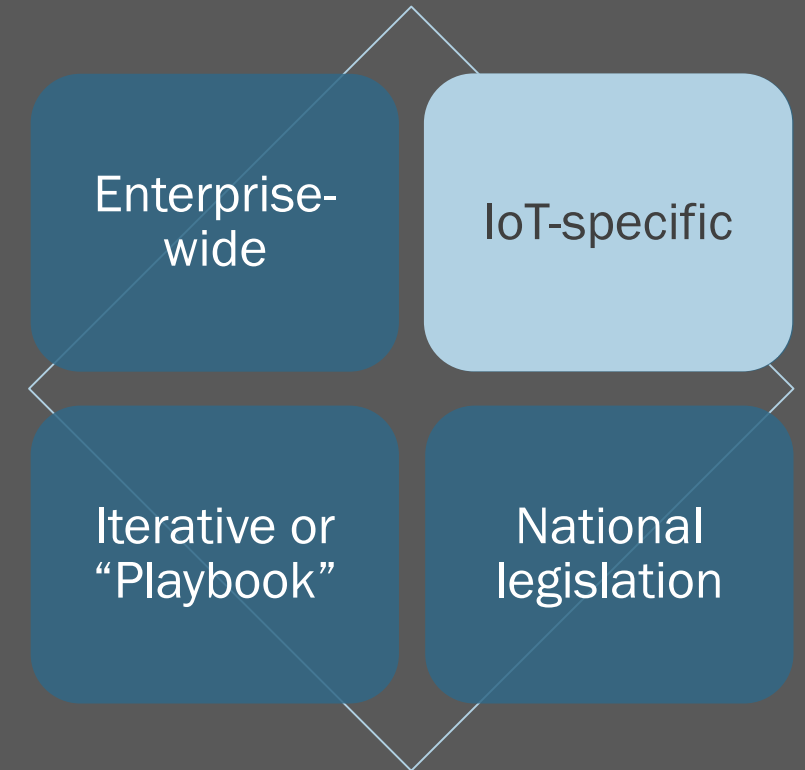
- General in nature
- Cuts across all city departments and all collection and use of data by the city
- Intended to act as a guidepost for many years of technological change
- Cities using this approach: Seattle



HARVARD
LAW SCHOOL

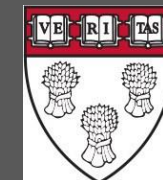
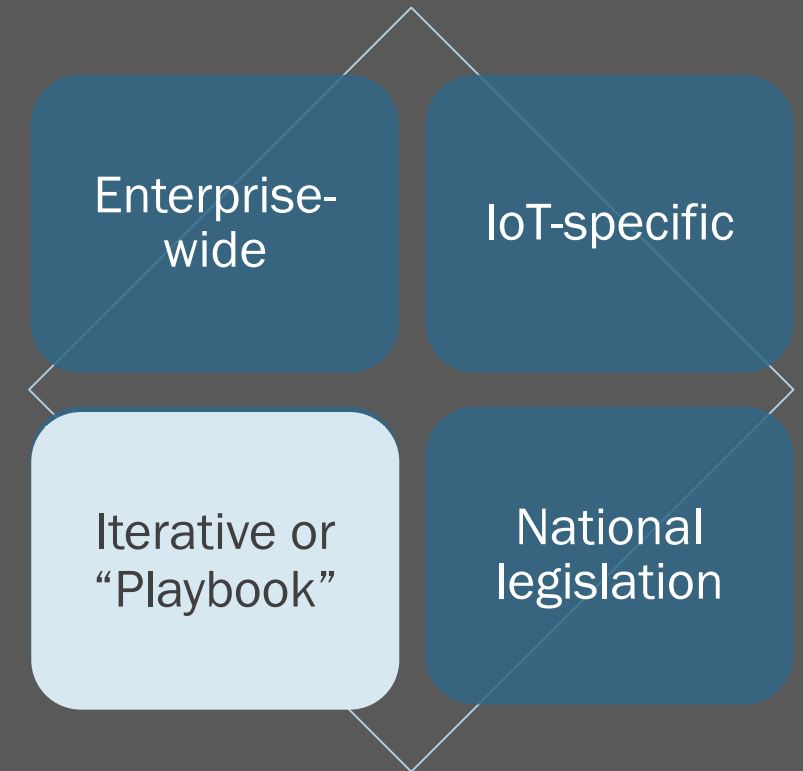
IoT-specific approach is focused.

- High-level, but designed with the context-specific attributes of IoT programs in mind
- Fewer practical challenges than Enterprise-wide approach
- Cities using this approach:
New York City



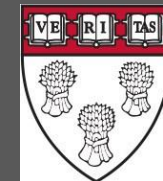
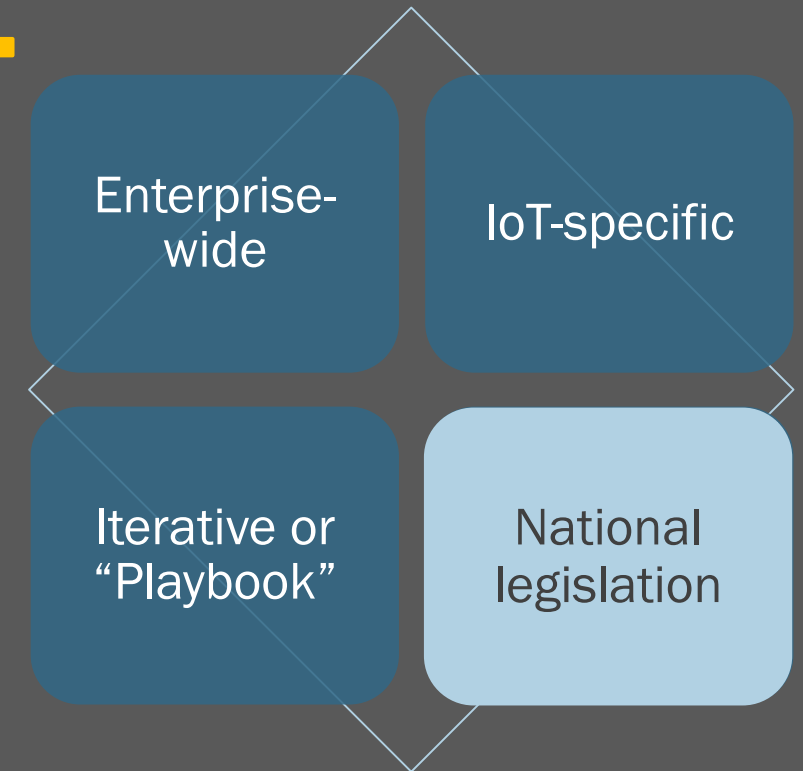
An iterative approach focuses on each project individually

- Desire to avoid “policy lock-in” and adapt approach as new technologies develop
- Broad principles might stifle innovation for fear of violating policy
- Cities using this approach: Austin, Boston, Philadelphia, Pittsburgh



Some municipalities are governed by national privacy legislation.

- Central to many international privacy regimes, especially in Europe
- Privacy principles are legally required to comply with enacted legislation
- Cities using this approach: Stockholm, London (for now)



We anticipate a 12 month timeline for Policy draft, engagement, and adoption.

Months 10-12

Finalize Digital Privacy & Security Policy
Plan Citywide rollout

Months 7-9

Synthesize findings and rework Policy
Develop plan for privacy governance model

Months 4-6

Draft Digital Privacy Policy
Engage external stakeholders and Council

Months 0-3

Engage cross-departmental and subject matter expert working group
Research other municipal approaches
Develop draft guiding principles

Many questions remain for us to consider...

- *Who owns the data?*
- *What is our retention policy?*
- *Where is it housed?*
- *Who are we sharing the data with?*
- *What is our monetization strategy?*
- *How are we managing Big Data?*
- *Chief Privacy Officer?*