Smart Cities Need Smart Data Privacy

Building Sustainable Smart Cities Through Data Governance

San Francisco Data Center Tech Conference and Expo

Smart Cities Raleigh Durham, North Carolina, USA

July 02, 2026 — Live Stream

SPEAKER: DEBBIE REYNOLDS, "THE DATA DIVA"

About Debbie Reynolds

Recognition

- Top 8 Global Data Privacy Expert
- Top 30 Global Risk Communicators
- Host of the #1 Global Data Privacy Podcast
- 1 Million + podcast downloads in 160+ countries

Leadership Roles

- Former Member, U.S. Department of Commerce IoT Advisory Board
- Chair, IEEE Global Trusted Data Architectures Industry Connections Subcommittee
- Speaker and advisor on privacy, AI, IoT, and data governance

> "Digital Systems Are Designed to Remember Data, Not to Forget it"
> — Debbie Reynolds, The Data Diva

Smart Cities Are Data Ecosystems

Every smart city initiative is also a data initiative. Data is the food of digital systems — smart cities are powered by connected data, and data privacy enables sustainable innovation.

Transportation & Mobility

- Intelligent transportation systems
- Smart parking & traffic signals
- Connected public transit
- EV charging infrastructure

Utilities & Environment

- Smart grids & street lighting
- Water, gas, electric utilities
- Air quality & flood monitoring
- Intelligent waste management

Citizen & Gov Services

- Digital citizen services
- Digital permitting & inspections
- Public safety & emergency response
- Fleet management & asset tracking

Example: Smart City Privacy Challenge: Smart Parking

A simple parking app illustrates how quickly data collection escalates. Every technology decision is also a data governance decision.

Parking Process

01

Scan QR code & download parking app

02

Create account & add payment method

03

Enter license plate; LPR records entry & exit

04

Parking session managed automatically

Data Collected & Privacy Risks

- Mobile device & account information
- Payment information
- License plate, entry & exit times
- Location and movement data

Privacy Considerations

- QR Code Security
- Data Minimization & Retention
- Location Privacy & Vendor Governance

The Five Privacy Questions Every Smart City Should Ask

1

Purpose

Why are we collecting this data?

2

Connection

What happens when this data connects with other systems?

3

Retention

How long should we keep this data?

4

Retirement

How do we securely retire the data and the device?

5

Innovation

How do we enable innovation while respecting privacy?

Why Are We Collecting This Data?

Data Collection Principles

- Define the business purpose
- Collect only what is needed
- Avoid overcollecting data "just in case"
- Review data collection as projects evolve
- Do not forget the end of the data lifecycle

Connected Data Creates New Data

Individual datasets may appear low risk, but connected datasets create new insights — and combined data increases privacy risk. Evaluate the entire data ecosystem.

High-Risk Data Combinations

- Parking + Transportation
- Public Safety + Cameras
- Citizen Apps + Mobility
- Utilities + Environmental Sensors

Retention, Deletion & Device Lifecycle

Data Privacy does not end when a device is retired.

Data Retention Principles

- Define retention requirements upfront
- Build deletion into the lifecycle
- Reduce unnecessary privacy risk
- Retention must support a business purpose

Secure the Entire Device Lifecycle

- Device sanitization
- Secure data deletion
- Asset retirement & recycling
- Vendor responsibilities

Privacy Enables Innovation

Good privacy practices support innovation and adoption. Privacy is not a barrier — it is the foundation of sustainable smart city design.

Privacy by Design

Embed privacy into systems from the start, not as an afterthought.

Governance by Design

Build accountability and oversight into every data initiative.

Transparency

Be clear with citizens about what data is collected and why.

Vendor Governance

Hold third-party vendors to the same privacy standards as internal teams.

U.S. DEPARTMENT OF COMMERCE | OCTOBER 2024

U.S. Department of Commerce IoT Advisory Board Recommendations (October 2024)

Use these recommendations to support planning, procurement, deployment, and lifecycle management of smart city technologies.

IoT Data Retention & Transparency

Establish clear policies for how long IoT data is kept and how it is disclosed.

Privacy by Design

Integrate privacy protections into system architecture from the outset.

Third-Party Data Governance

Require vendors to meet defined data governance and privacy standards.

Privacy Transparency Mechanisms

Provide accessible, clear notices to citizens about data collection practices.

Device & Media Sanitization

Ensure secure data deletion and device retirement at end of lifecycle.

DEBBIE REYNOLDS | "THE DATA DIVA" | DATADIVA.AI

The Data Diva's Smart City Privacy Checklist

Privacy is not a barrier to smart cities. Considering privacy is how smart cities become sustainable.

- Know **why** you are collecting the data.
- Understand what **connected data** can reveal.
- Define **retention** requirements before deployment.
- Plan for **deletion** and device sanitization.
- Build **privacy into every** smart city project.

> **Privacy is not a barrier to smart cities. Considering privacy is how smart cities become sustainable.**

Know why you are collecting the data.

Understand what connected data can reveal.

Define retention requirements before deployment.

Plan for deletion and device sanitization.

Build privacy into every smart city project.

Contact

Debbie Reynolds

Founder & CEO, Debbie Reynolds Consulting, LLC
Global Data Privacy & Emerging Technology Expert
Host, *The Data Diva Talks Privacy* Podcast

Email: dr@debbiereynoldsconsulting.com

Website: www.debbiereynoldsconsulting.com