Navigating Data Privacy in the Era of Smart Cities

Speaker: Debbie Reynolds

June 14, 2024
Debbie Reynolds  
Founder, CEO, and Chief Data Privacy Officer, Debbie Reynolds Consulting, LLC

- A leading voice in Data Privacy and Emerging Technology
- Hosts award-winning #1 “The Data Diva” Talks Privacy Podcast
- Recognized as one of the Global Top Eight Privacy Experts by Identity Review
- Named one of the Global Top 30 CyberRisk Communicators by The European Risk Policy Institute in 2020 and 2021
- Appointed to the U.S. Department of Commerce’s IoT Advisory Board in 2022
- Serves as the IEEE Committee Chair for Cyber Security for Next Generation Connectivity Systems at IEEE for Human Control & Flow
Data Growth

- 150X data growth by 2027
- 300X data growth by 2032
Data created over the next three years will be more than the data created over the past 30 years

(IDC Executive Summary- IDC's Global DataSphere Forecast 2020)
8.3 billion IoT devices were active in smart city projects globally in 2020.

https://gitnux.org/smart-city-statistics/
60% of the world’s population is expected to live in smart cities by 2050.
137 out of 194 countries have legislation to protect data and privacy.
IoT devices are typically attacked within five minutes of connecting to the Internet.

(NETSCOUT Threat Intelligence Report)
THE DATA PRIVACY CHALLENGES WITH SMART CITIES
Emerging Data

- New data types collected and retained
- Data about individuals' behavior being merged with other personally identifiable details
- Data about the biological features or reactions of a person
- Data that tracks the location of individuals
SMART CITIES
DATA COLLECTION AND USAGE

© Copyright 2024 Debbie Reynolds Consulting, LLC
Personal Data Types - GPS data, Biometric Data, Health Data, Surveillance Data, Financial Data, Emergency Data, etc.

Benefits / Usage - Enhance services, urban planning, sustainability

Data Collection Methods - IoT sensors, public databases, citizen apps

Data Retention - Capabilities, Requests, Regulations

Who is responsible? - Manufacturer, Implementer, Buyer, User
DATA PRIVACY
REGULATORY AND ETHICAL CONSIDERATIONS
Regulations and Ethics

- **Key Privacy Law Considerations** - Data Collection Transparency, Data Protection requirements, Data retention requirements
- **Methods to protect data** - Data minimization, privacy by design, purpose limitation
- **Compliance** - Adapting to evolving regulations
- **Ethics** - Would the data uses be deemed acceptable by the public?
Did you know there are Data Requirements that impact Smart City Tech?

- The U.S. Federal Trade Commission (FTC) considers Geolocation as “Sensitive Data” requiring increased protections (FTC ACT).
- In Illinois, biometric data retention is limited and can only be retained for three years after the last contact with the individual (Biometric Information Privacy Act - BIPA).
- In New Jersey, data of individuals must be removed from cars before resale (New Jersey Senate Bill S2740).
BEST PRACTICES FOR DATA PRIVACY IN SMART CITIES
Best Practices

- **Privacy by Design** - Integrate from the start regular assessments for high-risk data uses
- **Data Governance** - Clear policies, training, data stewardship
- **Technologies** - Encryption, Anonymization, Privacy Enhancing Technologies (PETs)
- **Engagement** - Educate municipalities, be transparent with citizens
Privacy Challenges - Understand issues in smart technologies

Regulations - Stay informed on data use / data limitation regulations

Minimization and Governance - Apply principles, ensure accountability

Technology Use - Implement PETs, encryption

Future Trends - Adapt to the evolving privacy landscape