Smart Cities: privacy and security

The concept of a 'smart city' has emerged out of a need for innovative urban design to cater for rapid increases in city populations around the world.[1] The use of information communications technology (ICT) in urban planning and design is projected to promote more efficient, convenient, economic and sustainable cities that meet the future needs of city dwellers. Such initiatives will require integration across many disparate systems and huge amounts of data (including personal information), making privacy and data protection vital considerations in establishing resilient cities aimed at ensuring long-term viability of resources and services, and creating public value.

What is a smart city?

A smart city uses technology to manage its resources, improve the way it delivers services, reduce costs and generate growth opportunities.[2] Typically, smart cities integrate ICT into innovative urban design to create a data-driven approach to public service delivery, infrastructure and public planning. Through the use of technology including smart devices, sensors, and the Internet of Things (IoT), citizens connect with industry and government and provide data to develop innovative ways to make urban areas more efficient, affordable, sustainable and ultimately, liveable.

Examples of smart city projects include:

- *environmental sensors* measuring real-time data on temperature, light, humidity, quality of air, water and soil
- *smart meters* providing real-time measurement of power, water, gas and energy consumption
- *smart LED street lighting* with street sensors and communication devices
- *automated waste management* through sensors detecting bin capacity
- *smart parking systems* sending nearby vacant parking alerts to drivers
- *smart irrigation systems* facilitating automated watering of parks
- *CCTV systems* for public safety, crowd management, and measuring the movement of people
- *smart cards* combining identification, transport and payment on one card
- *smart grids* combining communication, sensing and metering infrastructure with existing electricity networks
- *civic engagement platforms* to facilitate two-way communication between the city and citizens, to up-vote best ideas and crowd source creative solutions to existing problems.

Smart city benefits and objectives

The idea of a smart city can sometimes project a vision of a utopia in which an entire city has an 'operating system' that supports economic growth, environmental sustainability and improved liveability. Smart cities that employ privacy and security enhancing measures are likely to see the benefits of more open and transparent information sharing capacity, higher levels of trust from citizens and consumers, and a long-term sustainable trajectory that is committed to the creation of public value while being resistant to misuse.

Objectives and benefits of a smart city include:

- improving management of private and public transportation and efficient mobility
- environmental sustainability by monitoring and reducing waste through informed management of resources
- increased citizen participation through e-governance and participatory governance platforms
- coordinated emergency services and law enforcement responses
- fostering economic growth and improving quality and convenience of everyday life.

[1] Future projections indicate that cities will soon account for approximately 90% of population growth, 80% of wealth creation, and 60% of total energy consumption. Massachusetts Institute of Technology, 'About City Science', http://cities.media.mit.edu/about/cities

[2] Melbourne Networked Society Institute, 'Cities as living labs: Creating innovative, connected cities', Discussion paper, 2015, p. 3.

Privacy and security challenges and opportunities

Many initiatives mentioned above such as projects measuring the environment are unlikely to require personal information of citizens to function. Projects connecting personal ICT or IoT devices to a city network, or that use CCTV or any form of identification system, will require the collection, use and potential disclosure of personal information. Security risk management procedures are integral to handling *any* public sector information, and both privacy and security protections are essential to mitigate potential breaches including *personal* information. Making privacy and security considerations from the outset offer the opportunity to build robust foundations for smart city innovation. Public trust and public value can be increased by ensuring that personal information of citizens will be kept secure, and not subject to avoidable risk or misuse. This, in turn, promotes long-term viability of projects.

Highlighted below are some of the key privacy and data protection considerations for smart cities. With each challenge there are a number of ways in which negative effects can be reduced, resulting in smart city initiatives that enhance both privacy and information security.

Data collection The ICT used to enable smart cities has the ability to gather unprecedented amounts of data about citizens. Properly managing and protecting this data is integral to mitigating privacy and security risks. Limiting the collection of personal information to that which is necessary to achieve the desired outcome of an initiative is a critical step.

Information sharing Smart cities are based on connectivity, requiring increased information sharing both within the public sector and with external entities. Many large datasets will be linked or released through open data platforms. Ongoing information sharing agreements combined with techniques such as de-identification are useful to enhance citizens' privacy.

Security risk management Security controls that go beyond just ICT solutions will help mitigate potential incidents. Technical solutions such as encryption, digital signature and server reliability are important, as are defined document policies, procedures, incident and risk management protocols, physical security, and personnel training and awareness.

Malicious attacks If an entire city is connected and has an 'operating system' containing vast amounts of personal information and with control of critical infrastructure, there may be incentive for a malicious intruder to seek unauthorised access. Implementing security risk management procedures as highlighted above can help mitigate these risks.

Human error Human error, intentional or accidental, can elevate risk of privacy and security breaches. This is often the result of lack of training, oversight practices and access controls. Those with access to personal information need to understand their responsibilities and act in accordance with policies and procedures.

Chilling effect Where individuals feel they are being monitored, there is potential for change of behaviour known as the 'chilling effect'. This is largely due to a lack of trust that collected information will be used appropriately. There are several avenues to alleviate this concern including obtaining consent, giving notice of data collection, and providing the option of anonymity or opting-out. It is also widely suggested that smart cities should be 'citizen-led' to increase public participation and maintain trust between citizens, the public sector and the private sector.[3]

Governance Initiating a smart city raises questions as to who will have ownership over the technology, data and its management. Strong leadership, clear policies, procedures and guidance, accountability, transparency, and a commitment to privacy and security by design will be fundamental regardless if smart cities are lead by the public or private sector.

[3] Nicole Kobie, 'Why smart cities need to get wide to security – and fast', The Guardian, 13 May 2015, http://www.theguardian.com/technology/2015/may/13/smart-cities-internet-things-security-cesar-cerrudo-ioactive-labs

Commissioner for Privacy and Data Protection

Background paper