Getting smarter about smart cities:
Improving data privacy and data security

Department of the Taoiseach

The Programmable City

NIRSA

Getting smarter about smart cities: Improving data privacy and data security

Published by:
Department of the Taoiseach on behalf of the Government Data Forum, January 28th 2016

Authored by:
Rob Kitchin, NIRSA, Maynooth University

Suggested citation:
Kitchin, R. (2016) *Getting smarter about smart cities: Improving data privacy and data security*. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Minister's Foreword

It gives me great pleasure to present this report 'Getting smarter about smart cities: Improving data privacy and data security'.

The report is the first publication from the Government Data Forum, a group that brings together experts from across a wide range of sectors including researchers, industry, civil society, legal experts and the public sector to examine the data privacy and protection challenges posed by the digital age. The Forum is the first of its kind internationally to gather together such a wide range of stakeholders to contribute to the wider debate that we need to have as a society about our data. We need to look at how we use them, what we exchange for them, the great uses they can be put to - if handled correctly - to improve our lives and help address some of the big challenges we face, and the norms that we will settle on and accept as technology develops further.

Ireland is uniquely well-placed to harness the potential of data. We have many of the world's top technology and data focused multinationals on these shores, a thriving indigenous technology enterprise sector, and excellent collaboration between academic research institutions and industry, underpinned by a targeted approach by Government to support science and innovation.

This report, commissioned from Professor Rob Kitchin of the National Institute for Regional and Spatial Analysis (NIRSA) at Maynooth University, provides an excellent overview of the innovative technological approaches that are been taken internationally in the management of Smart Cities.

The report serves as a reminder that Smart Cities bring huge potential benefits in producing more efficient, productive, sustainable, resilient, transparent, fair and equitable cities. We need to ensure that we carve a path that allows us to harness these benefits while at the same time, ensuring that we do not compromise data privacy, data protection or data security. Having read this report and its recommendations, I am confident that we can do this, and that Ireland can set an example internationally in embracing these emerging technologies while creating a trusted, transparent and balanced environment.

Dara Murphy T.D.
Minister for European Affairs and Data Protection
Chair of Government Data Forum

Table of Contents

List of Acronyms

AIS	Automation Identification System
ANPR	Automatic Number Plate Recognition
API	Application Program Interface
ATM	Automatic Teller Machine
BSSID	Basic Service Set Identifier
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
CDO	Chief Data Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CLI	Command Line Interface
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CRM	Customer Relations Management
CSIRT	Computer Security Incident Response Team
CTO	Chief Technology Officer
DoS	Denial of Service
EOS	Energy Optimisation System
EPA	Environmental Protection Agency
EU	European Union
FAA	Federal Aviation Administration
GPS	Global Positioning System
GSM	Global System for Mobile communication
FBI	Federal Bureau of Investigation
FIPPS	Fair Information Practice Principles
FOGMON	Fats, Oils and Grease Monitoring
FTC	Federal Trade Commission
HVAC	Heating, Ventilation and Air Conditioning

ICS	Industrial Control Systems
ICT	Information and Communication Technologies
ID	Identifier
IMEI	International Mobile Station Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LTE	Long Term Evolution
MAC	Media Access Control
MEID	Mobile Equipment Identifier
MMS	Multimedia Messaging Service
NCSC	National Cyber Security Centre
NFC	Near-Field Communication
NSBET	National Sustainable Energy Testbed
NDRC	National Digital Research Centre
OECD	Organisation for Economic Co-operation and Development
OS	Operating System
PAC	Privacy Advisory Committee
PETS	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIR	Private Information Retrieval
PPDM	Privacy-Preserving Data Mining
RFID	Radio Frequency Identifier
RSSI	Received Signal Strength Indicator
SCADA	Supervisory Control and Data Acquisition
SCATS	Sydney Coordinated Adaptive Traffic System

SDC	Statistical Disclosure Control
SDK	Software Development Kit
SEAI	Sustainable Energy Authority of Ireland
SIM	Subscriber Identity Module
SFI	Science Foundation Ireland
SME	Small and Medium Enterprises
SMS	Short Message Service
SQL	Structured Query Language
SSID	Service Set Identifier
TfL	Transport for London
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Universal Resource Locator
US	United States

Executive summary

Many cities around the world are seeking to become a smart city, using networked, digital technologies and urban big data to tackle a range of issues, such as improving governance and service delivery, creating more resilient critical infrastructure, growing the local economy, becoming more sustainable, producing better mobility, gaining transparency and accountability, enhancing quality of life, and increasing safety and security. In short, the desire is to use digital technology to improve the lives of citizens, finesse city management, and create economic development.

In this context, a wide range of smart city technologies are being deployed within urban environments, including city operating systems, centralised control rooms, urban dashboards, intelligent transport systems, integrated travel ticketing, bike share schemes, real-time passenger information displays, logistics management systems, smart energy grids, controllable lighting, smart meters, sensor networks, building management systems, and an array of smartphone apps and sharing economy platforms. All of these technologies generate huge quantities of data, much of them in real-time and at a highly granular scale.

These data about cities and their citizens can be put to many good uses and, if shared, for uses beyond the system and purposes for which they were generated. Collectively, these data create the evidence base to run cities more efficiently, productively, sustainably, transparently and fairly. However, generating, processing, analysing, sharing and storing large amounts of actionable data also raise a number of concerns and challenges.

Key amongst these are the data privacy, data protection, and data security issues that arise from the creation of smart cities. Many smart city technologies capture personally identifiable information (PII) and household level data about citizens – their characteristics, their location and movements, and their activities – link these data together to produce new derived data, and use them to create profiles of people and places and to make decisions about them. As such, there are concerns about what a smart city means for people's privacy and what privacy harms might arise from the sharing, analysis and misuse of urban big data. In addition, there are questions as to how secure smart city technologies and the data they generate are from hacking and theft and what the implications of a data breach are for citizens. While successful cyberattacks on cities are still relatively rare, it is clear that smart city technologies raise a number of cybersecurity concerns that require attention.

To date, the approach to these issues has been haphazard and uncoordinated due to the ad-hoc manner in which they were developed. However, given the potential harms to citizens and the associated costs that can arise, and the potential benefits at stake, this approach should not be allowed to continue. The challenge is to rollout smart city solutions and gain the benefits of their deployment while maintaining infrastructure and system security and systematically minimising any pernicious effects and harms. This is no easy task, given the many stakeholders and vested interests involved and their differing aims and ambitions, and the diverse set of technologies and their complex arrangement.

This report details the development of smart cities and urban big data, highlights the various privacy and security concerns and harms related to the deployment and use of smart city technologies and initiatives, and makes a number of suggestions for addressing trepidations about and ills arising from data privacy, protection and security issues.

It argues that there is no single solution for ensuring that the benefits of creating smart cities are realised and any negative effects are neutralised. Rather, it advocates a multi-pronged approach that uses a suite of solutions, some of which are market driven, some more technical in nature (privacy enhancement technologies), others more policy, regulatory and legally focused (revised fair information practice principles, privacy by design, security by design, education and training), and some more governance and management orientated (at three levels: vision and strategy – smart city advisory board and smart city strategy; oversight of delivery and compliance – smart city governance, ethics and security oversight committee; and day-to-day delivery – core privacy/security team, smart city privacy/security assessments, and computer emergency response team).

These solutions provide a balanced, pragmatic approach that enable the rollout of smart city technologies and initiatives, but in a way that is not prejudicial to people's privacy, actively work to minimise privacy harms, curtail data breaches, and tackle cybersecurity issues. They also work across the entire life-cycle (from procurement to decommissioning) and span the whole system ecology (all its stakeholders and components). Collectively they promote fairness and equity, protect citizens and cities from harms, and enable improved governance and economic development. Moreover, they do so using an approach that is not heavy handed in nature and is relatively inexpensive to implement. They are by no means definitive, but build on and extend work to date, advance the debate, and detail a practical route forward.

The report concludes that a core requirement for creating smart cities is the adoption of an ethical, principle-led approach designed to best serve the interests of citizens. In other words, being smart about how we plan and run cities consists of much more than deploying data-driven, networked technologies; it requires a smart approach.

1. Smart cities

In recent years, many cities have declared their intention to become 'smart cities', initiating smart city programmes and deploying smart city technologies. A plethora of companies have begun to market smart city solutions. They have been joined by a range of governmental and supra-national initiatives and funding programmes, industry think-tanks and lobby groups, non-governmental organisations and university research centres, focused on promoting and developing smart cities. Yet, as with many technology-related buzz phrases, the term 'smart city' lacks a well delineated and agreed upon definition.

A review of the academic, stakeholder and corporate literature reveals that a smart city is comprehended in three broad ways. In each case, the vision is building upon earlier initiatives and technological deployments which have been in progress from the early 1970s (e.g., cybernetic cities, wired cities, cyber cities, digital cities, knowledge cities, intelligent cities, innovation cities) and overlap with other popular, current city framings (e.g., resilient cities, sustainable cities, safe cities, eco-cities).[1]

First, there is a constituency that understands smart cities to be principally about digitally instrumenting cities to change how urban infrastructures and city services are configured and managed. In this vision, the city is increasingly composed of networked, digitally-enabled devices directly embedded into the fabric of cities (e.g., digital CCTV, smart meters, transponders, sensor networks, software-controlled equipment, etc.) that produce continuous streams of data that dynamically feed into management software and control rooms enabling the real-time regulation of city systems (e.g., transport management, energy supply, emergency services; see Table 1).[2] These are supplemented by new media such as smartphone apps that both present and generate a range of information about the city and its citizens. These data-driven, networked technologies work to make cities knowable and controllable in new, dynamic, reactive ways through the use of vast quantities of real-time data and interactive, programmable systems.[3] Moreover, the data generated can be used to create and improve models and simulations to guide future urban development.[4]

Second, there are some who conceive of the smart city as an initiative principally concerned with improving urban policy, development and governance by using advances in ICT to reconfigure human capital, creativity, innovation, education, participation, sustainability, and management.[5] Here, it is envisioned that the strategic use of ICT produces smarter citizens, workers and public servants that in turn can enact smarter policy and programmes, produce better products, foster indigenous entrepreneurship and attract inward investment. A smart city is thus one that utilises e-government, publishes open data and fosters an open data economy, creates citizen-centric dashboards about city performance, encourages citizen participation in reporting issues and planning, enables urban test-bedding (wherein companies can trial new technologies aimed at improving urban services), actively nurtures start-up companies and accelerator programmes, promotes the use of ICT in education programmes, and actively leverages the technologies and data detailed in

Table 1 to create new synergies, especially cross-sectoral approaches that break down departmental silos.

Table 1: Smart city technologies

Domain	Example technologies
Government	E-government systems; online transactions; city operating systems; performance management systems; urban dashboards
Security and emergency services	Centralised control rooms; digital surveillance; predictive policing; coordinated emergency response
Transport	Intelligent transport systems; integrated ticketing; smart travel cards; bikeshare; real-time passenger information; smart parking; logistics management; transport apps
Energy	Smart grids; smart meters; energy usage apps; smart lighting
Waste	Compactor bins and dynamic routing/collection
Environment	Sensor networks (e.g., pollution, noise, weather; land movement; flood management)
Buildings	Building management systems; sensor networks
Homes	Smart meters; app controlled smart appliances

A third conception of a smart city is one that uses digital technologies and ICT to promote a citizen-centric model of urban development and management that promotes social innovation and social justice, civic engagement and hactivism, and transparent and accountable governance.[6] A smart city thus promotes a smart society that provides equal opportunities, serves local communities, and reduces inequalities. Here, there is an emphasis on fostering civic hacking and hackathons; participatory planning and community development; open source platforms, software and data; freedom of information; crowd sourcing and communal action; and digital and data literacy. This conception of a smart city is forwarded as either a counter-weight to the first two, or as an alternative.

For many stakeholders, these three conceptions of a smart city are not mutually exclusive, with smart city strategies seeking to blend elements from all three in varying proportions and with different priorities. Indeed, it is important to recognise that the underlying visions, ambitions and drivers of smart cities vary between places.[7] For example, in Europe/US the development of smart cities is principally concerned with improving the efficiency of city services, creating resilience and sustainability, strengthening security and control, and fostering economic development. In China, India and Africa, smart city initiatives are promoted as a way of enabling modernisation and national development, responding to population growth/migration, and managing economic and urban transitions. Within these broad geographic areas, there is considerable variation depending on the priorities of city governments and administrations, and the influence of local culture, history, politics and

economies. Moreover, while most smart city initiatives are concerned with retro-fitting existing cities, some cities or new city districts are being created from scratch as smart cities (e.g., Songdo in South Korea, Masdar in the United Arab Emirates, and a large number of the 100 planned smart cities in India).

Despite variations in smart city visions and deployments, each is united through an expectation that data-driven, networked technologies can be used to reconfigure how aspects of daily life are performed for the better and to tackle pressing urban issues, producing a:

- *smart economy* by fostering entrepreneurship, innovation, productivity, and competiveness;
- *smart government* by enabling new forms of e-government, new modes of operational governance, improved models and simulations to guide future development, evidence-informed decision making, better service delivery, and making government more transparent, participatory and accountable;
- *smart mobility* by creating intelligent transport systems and efficient, inter-operable multi-modal public transport;
- *smart environments* by promoting sustainability and resilience and the development of green energy;
- *smart living* by improving quality of life, increasing safety and security, and reducing risk; and
- *smart people* by creating a more informed citizenry and fostering creativity, inclusivity, empowerment and participation.[8]

In short, producing smart cities promises to solve a fundamental conundrum of cities – how to reduce costs and create economic growth and resilience at the same time as producing sustainability and improving services, and increasing participation and quality of life – and to do so in commonsensical, pragmatic, neutral and apolitical ways through the use of data-driven, networked solutions.[9]

2. Irish cities as smart cities

The four principal Irish cities – Dublin, Cork, Galway and Limerick – have all deployed smart city technologies, though they vary in the scale of rollout and the extent to which they are coordinated through a smart city vision. Dublin and Cork have most enthusiastically embraced the notion of becoming smart cities and both have smart city strategies: Smart Dublin (www.smartdublin.ie) and Cork Smart Gateway (www.corksmartgateway.ie/). In both cases, the vision of smart cities is a mix of data-driven, networked infrastructure, fostering economic growth and entrepreneurship, and citizen-centric initiatives, with a particular focus on creating more efficient city services, improved transportation flows, tackling flooding, attracting inward investment and encouraging indigenous start-ups and SMEs, and open data and civic engagement. Initiatives concerning security and policing, which are more prominent in UK and US cities where terrorism is seen as more of a threat, are less of a priority.

In the case of Irish cities, all initiatives are building on top of legacy infrastructure and many decades of social and economic programmes, rather than creating new, from the ground-up smart city districts. As such, smart city initiatives and technologies have to be layered on top of long standing systems and schemes, and be accommodated within or replace existing organisational structures. Nonetheless, an audit of the four Dublin local authorities (Dublin City Council, Dun Laoghaire-Rathdown County Council, South Dublin County Council, Fingal County Council) and the two Cork local authorities (Cork City Council, Cork County Council) reveals a relatively large number of mainstreamed smart city initiatives (see Tables 2 and 3).

In the case of Dublin, there is a whole raft of smart city apps available, some provided/commissioned by local authorities (e.g., Art Trax, Heritage Walks, Mindmindr), others developed by citizens and commercial enterprises (e.g., Hit the Road, Parkya, Walk Dublin[10]) beyond the initiatives detailed in Table 2. Moreover, there is a range of on-going research and pilot projects that have yet to be mainstreamed, and others that ran for a handful of years before terminating. Further, beyond the economic development organisations listed in Table 2, there is a fairly well developed ecosystem of 'university-industry-local government' smart city research centres and collaborations (including 'The Programmable City' (implications of creating smart cities), 'Innovation Value Institute' (business models for smart city technologies), 'Insight' (data analytics for smart cities), 'CONNECT' (networking and comms for smart cities), 'Future Cities' (sensor, communication and analytical technological solutions for sustainability), 'Dublin Energy Lab' (smart grids and meters)) and some industry centres (e.g., IBM's smart city global research team) and test-beds (especially relating to the Internet of Things). Organisations such as Codema and Sustainable Energy Authority of Ireland (SEAI) undertake smart energy/grid projects and provide advice and guidance. In other words, Dublin can lay claim to being a nascent smart city, rather than simply trying to become one.

Table 2: Smart Dublin

Smart economy	Dublinked	Provides access to city datasets, including to some real-time data feeds
	Digital Hub	Cluster of digital content and technology enterprises; provides space, infrastructure and support services for digital tech companies
	Startup Commissioner	Advocates for tech start-ups; organises events and support schemes
	NDRC	Provides supports and capital investment for start-ups; runs/sponsors hackathons
	Greenway	Cleantech cluster supporting and developing the green economy
Smart government	Fix-your-street	A website and app for reporting issues (e.g., vandalism, dumping, potholes) to local authorities
	Public realm operations map	An interactive map that reports where and how local authority funds are spent
	CRM workflow	Customer relations management system used to interface with the public and undertake workflow planning
	Library digital services	A suite of library apps for various services
	Intelligent transport system	A suite of different technologies including SCATS (transduction loops at junctions), CCTV, ANPR (automatic number plate recognition cameras), detection of breaking red lights at Luas (tram) lines, feeding into a centralised traffic control room
	Eflow road tolling	Automated roll tolling/billing using transponders
	Fleet management	GPS tracking of local authority fleets and route optimisation
Smart living	Street CCTV	Network of digital interactive CCTV cameras (alter direction/zoom)
	Community CCTV	Network of CCTV in public places (e.g., parks); provides SMS alerts; can communicate through speakers in lampposts
	Sonitus sound sensing	Network of sound sensors monitoring noise levels
	Monitored sheltered housing	Remote monitoring of movement sensors and panic buttons in sheltered homes
	Smart Stadium	Sensor network monitoring different facets of stadium use

Smart mobility	Leapcard	Smart card access/payment for trains, buses and trams.
	Real-time passenger information	Digital displays at bus and tram stops and train stations providing information on the arrival/departure time of services
	Smart parking	Transponder payment system; park-by-text; display around city; API feed
	Information display signs	Traffic (crash/delay) alerts; speeding display signs
	Bliptracker displays	Bike counters; car parking spaces counters; airport queue counters
	Dublin Bikes	Public hire bike scheme
Smart environment	Sensor flood monitoring	Use of sensor network to monitor river levels by the Environment Protection Agency (EPA) and local authorities
	Pollution monitoring	EPA network of pollution sensors
	Public building energy use	Real-time monitoring of energy use with local authority buildings; publicly displayed on screens
	Big Belly Bins	Networked compactor bins that use sensors to monitor waste levels; waste collection route optimisation
Smart people	DublinDashboard	Comprehensive set of interactive graphs and maps of city data, including real-time data, as well location-based services
	Fingal Open Data	Local authority open data sets
	Map Alerter	Real-time alerts of weather and flooding
	CIVIQ	Consultation and deliberation tool for planning and development
	Citizenspace	Consultation and deliberation tool for planning and development
	Tog	Civic hacking maker meetups
	Code for Ireland	Civic hacking coding meetups

Source: Coletta, Heaphy and Kitchin (2015); only includes operational, rolled-out initiatives procured or co-developed by local authorities

Likewise, in Cork a 'smart agenda' is being developed that builds on the existing assets, attributes and experiences in the region through the 'Cork Smart Gateway' initiative, which is a collaboration between the two local authorities and the Nimbus Research Centre (Internet of Things, networks) and Tyndall National Institute (ICT, microelectronic circuits, nanotechnology, energy, photonics). The aim is to leverage a quadruple helix innovation model where government, industry, academia and civil participants work together to co-create and drive structural change utilising ICT solutions. As well as a host of EU, SFI and enterprise projects, Cork is also home to the National Sustainable Building Energy Testbed, Water Systems and Service and Innovation Centre, and the Mallow Systems and Innovation Centre, and UCC is a lead partner of Insight and CONNECT.

In addition to these projects, Cork City Council is a follower City in a Smart Cities and Communities Horizon 2020 project called GrowSmarter, a €25m initiative (lead cities: Stockholm, Cologne, and Barcelona). GrowSmarter establishes three 'lighthouses' for smart cities which demonstrate to other cities how they can be prepared in an intelligent way for the energy challenges of the future. As part of this project, Cork will roll out initiatives in transport, energy, and information and communications technology. There are also a significant number of companies driving Internet of Things development in the region, for example, EMC and Vodafone have jointly invested €2m in a new INFINITE internet of things industrial platform that will traverse Cork.

Table 3: Smart Cork

Smart economy	Energy Cork	Cluster supporting collaboration and innovation in the energy sector
	IT@Cork	Cluster supporting collaboration and innovation in the ICT sector
	TEC Gateway – part of Nimbus, CIT	EI funded technology gateway supporting Irish industry to develop new IoT technologies
	Rubicon	Incubator – provides supports and capital investment for startups
Smart government	City Council housing stock management	Stock condition surveys and maintenance activities updated by smart technologies close to real time
	Library digital services	A suite of library apps for various services
	Variable messaging signs	Real time off-street parking and road closure information on key access routes to the city
Smart living	Smart energy management	Real-time monitoring and control of energy use and environmental characteristics for residential and commercial buildings; Secure management and prognostics networks for energy systems – EOS

	Smart urban district energy Management	Real-time monitoring and control of neighbourhoods (blocks of buildings) for sustainable energy use
	Smart lighting	Intelligent LED lighting networks
	GreenCom	Smart microgrid testbed that enables wireless monitoring/control of loads, microgeneration and microstorage energy elements
Smart mobility	Coca Cola Zero Bikes	Public Hire Bike Scheme
	LeapCard	Smart card access/payment for trains and buses
	Real-time passenger information	Real time bus and train information at stops
	EV Infrastructure	Deploy standard and fast charging points throughout the city
Smart environment	Smart testbeds	National Sustainable Energy Testbed (NSBET); Community Testbed - A regional community testbed with access to high-performance broadband facilities; Water Test-bed
	River Lee deployment	Real time wireless sensor river monitoring system looking at water quality and depth
	Rainwater harvesting	Remote monitoring of rainwater harvesting system in Sunview Fairhill
	Smart water	Sensor development and integration to support management of Fats, oils and greases in the waste water networks – FOGMON Aquametrics – Single point monitoring of water networks
	Mid-altitude security and environmental monitoring	AEOLUS – Mid-altitude (400m) sensor platform combining HD cameras, metrological, Radar and AIS for coastal monitoring for security and environmental assessment
Smart people	Maker Dojo	Hands-on, 'hacker' style workshops
	CorkCitiEngage	A Cork Smart Gateway Survey Project. Public feedback on public issues, digital skills, and use of public infrastructure
	CorkOpenData	data.corkcity.ie – An online platform for publishing city information obtained from various sources, from sensors to surveys

Source: Compiled by the Cork Smart Gateway

3. Urban big data and open data

Central to the creation of smart cities is the generating, processing, analysing and sharing of vast quantities of data about city infrastructure, services, and citizens. Indeed, smart cities technologies are precisely about making cities data-driven: enabling city systems and services to be responsive to and act upon data, preferably real-time data.[11] It is thus no coincidence that the drive to create smart cities dovetails with the unfolding data revolution.[12] This revolution consists of five main elements:[13]

1. the wide scale production of big data: data that are continuously produced, exhaustive to a system, fine-scaled, relational, and flexible;
2. the scaling of traditional small data into data infrastructures (digital repositories), enabling datasets to be shared, conjoined and analysed in new ways;
3. the creation of linked data that seeks to transform the internet into a 'web of data', enabling all documents to be rendered as data and to be harvested and linked together;
4. the publishing of open data, making data publicly available and free to use that was previously locked inside institutions;
5. the development of new data analytics that often rely on machine learning techniques which can cope with and draw insight from very large datasets (e.g., data mining and pattern recognition; data visualisation and visual analytics; statistical analysis; and prediction, simulation, and optimisation modelling).

Nearly all of the technologies listed in Tables 1, 2 and 3 are data-driven – producing, deriving value from, and acting on data. Most are producing urban big data of varying kinds.[14] Four are explicitly open data infrastructures (CorkOpenData, Dublinked, Fingal Open Data, Dublin Dashboard). Many of them have accompanying apps (that further leverage the data and which can themselves produce further data) and APIs (that enable the data to be accessed and repurposed).

In addition to the big data generated by the initiatives detailed in Tables 2 and 3, a deluge of other big and open data are being produced with respect to Dublin, Cork and other cities in Ireland and around the world by a range of public and private organisations:

- utility companies (use of electricity, gas, water, lighting);
- transport providers (location/movement, traffic flow);
- mobile phone operators (location/movement, app use, behaviour);
- travel and accommodation websites (reviews, location/movement, consumption);
- social media sites (opinions, photos, personal info, location/movement);
- crowdsourcing and citizen science (maps (e.g., OpenStreetMap), local knowledge (e.g., Wikipedia), weather (e.g., Wunderground));
- government bodies and public administration (services, performance, surveys);

- libraries, museums, broadcasters, archives (history of people, cultures and places);
- financial institutions and retail chains (consumption, location);
- private surveillance and security firms (location, behaviour);
- emergency services (security, crime, policing, response); and
- home appliances and entertainment systems (behaviour, consumption).

While much of these data are closed and considered a private asset, some of them are shared with third party vendors and some are open (through data infrastructures or APIs). All these data can be potentially leveraged to create smart city technologies with respect to the six domains set out in column 1 of Tables 2 and 3.

Smart city initiatives such as urban operating systems (sometime called Urban OS or City OS) seek to link together multiple smart city technologies to enable greater coordination of city systems. Similarly, urban operating centres and urban dashboards attempt to draw and link as much of their data together to provide synoptic city intelligence (see Boxes 1 and 2). The abundance of data and new analytics are also helping to create new analytical fields such as urban informatics (an informational and human-computer interaction approach to examining and communicating urban processes) and urban science (a computational modelling and simulation approach to understanding, explaining and predicting city processes).

Box 1: Urban Operations Centre

The Centro De Operacoes Prefeitura Do Rio is a purpose built urban operations centre. Part of the impetus for the centre was to create a command and control hub for managing city operations in the lead up to and during three major sporting events: The Confederations Cup; The World Cup; and the Olympics. More generally, it was built to aid the city administration in managing and controlling a large, diverse, complex city, and in the words of the city mayor, Eduardo Paes, "to knock down silos … [between] departments and combine each one's data to help the whole enterprise."[15] It is operated on a twenty four hour basis, seven days a week, and is staffed by 400 professional workers employed over three shifts.[16]

The centre draws together data streams from thirty agencies, including traffic and public transport, municipal and utility services, emergency services, weather feeds, social media, and information sent in by the public via phone, internet and radio. This is complemented by a virtual operations platform accessible by mobile devices that enable city officials to log-in from the field to access real-time information. For example, police at an accident scene can use the platform to see how many ambulances have been dispatched and when, and to upload additional information.[17]

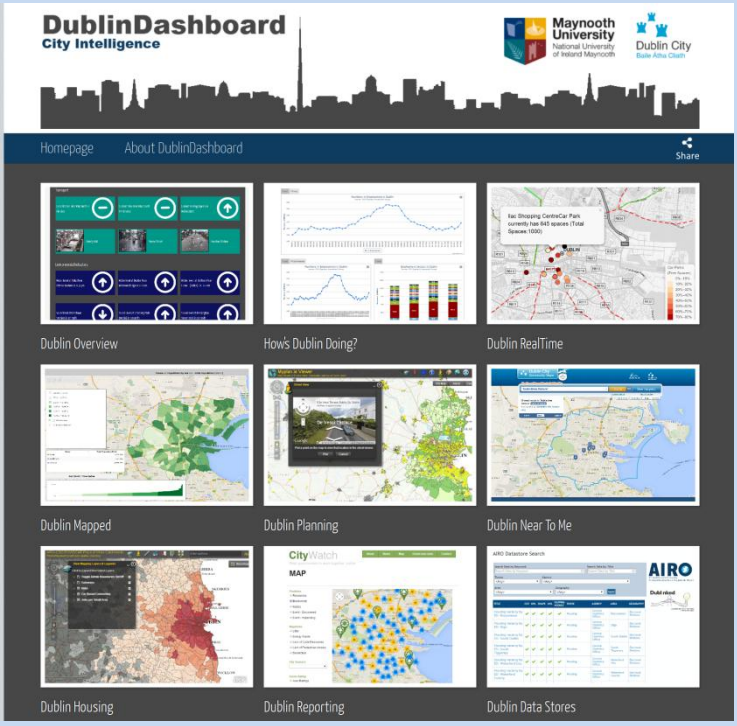
In the centre a team of analysts, aided by various data analytics software, process, visualise, analyse and monitor the vast deluge of live service data, alongside data aggregated over time and huge volumes of public administration data that are released on a more periodic basis. The data are used for real-time decision making and problem solving. Moreover, data can be mashed together to investigate particular aspects of city life and change over time, and to build predictive models with respect to everyday city development and management and disaster situations such as flooding. In cases of emergencies, the centre becomes a crisis management centre.[18]

Given that the centre is live tracking events across the city it has also become a media centre, used to produce live traffic and local news updates. Some of these, along with some of the live data, are viewable on the centre's website.

Centro De Operacoes Prefeitura Do Rio in Rio de Janeiro, Brazil, www.centrodeoperacoes.rio.gov.br

Box 2: Urban Dashboard

The Dublin Dashboard is an interactive website and portal that provides access to a wide range of datasets about the city and a suite of visualisation and analysis tools. It is designed to enable users to gain detailed, up-to-date intelligence about the city that aids everyday decision making and fosters evidence-informed analysis.



The underlying data is drawn together from the four Dublin local authorities, Dublinked, Central Statistics Office, Eurostat, and government departments. These data are displayed through hundreds of interactive data visualisations. However, no personably identifiable information is displayed.

The site consists of several modules, each of which contains a number of apps. Users can:

- examine how Dublin is performing on a number of metrics and compared to other cities and regions;
- see how local authorities spend their budget;
- view what is happening with transport and the environment in real-time;
- interact with maps of the Census, crime, live register, companies, housing, and planning;
- find city services near to them;
- report issues in their area; and
- download data to conduct their own analysis or build apps

The site was designed so that: all available open data about the city, including real-time data, is made available; there are no closed elements; it is very easy to use, with users requiring no mapping or graphing skills; all the apps are interactive so that users can explore the data; and existing resources and apps are used so that there is no duplication of effort.

Dublin Dashboard, www.dublindashboard.ie

4. The perils of smart cities and data-driven urbanism

The promises of smart cities are alluring and there is no doubt that smart city technologies help to create cities that are more efficient, competitive, productive, sustainable, resilient, participatory and transparent. That said, the drive to create smart cities also raises a number of concerns and risks, which can be classified into eight broad types:[19]

1. It typically treats the city as a knowable, rational, steerable machine, rather than a complex system full of wicked problems and competing interests;[20]
2. It promotes a strong emphasis on creating technical solutions and overly promotes top-down technocratic forms of governance, rather than political/social solutions and citizen-centred deliberative democracy;[21]
3. The technological solutions forwarded often treat cities as ahistorical and aspatial and as generic markets, promoting one-size fits all technical fixes rather than recognising the need for bespoke solutions tailored to city characteristics and needs;[22]
4. The technologies deployed are portrayed as being objective, commonsensical, pragmatic and politically benign, rather than thoroughly political, reflecting the views and values of their developers and stakeholders;[23]
5. It promotes the corporatisation and privatisation of city services, with the developers of smart city technologies capturing city functions as market opportunities which are run for profit rather than the public good, and potentially create propriety technological lock-ins;[24]
6. It prioritises the values and investments of vested interests, reinforces inequalities, and deepens levels of control and regulation, rather than creating a more socially just and equal society;[25]
7. The technologies deployed have profound social, political and ethical effects: introducing new forms of social regulation, control and governance; extending surveillance and eroding privacy; and enabling predictive profiling, social sorting and behavioural nudging;[26]
8. The technologies deployed potentially produce buggy, brittle and hackable urban systems which create systemic vulnerabilities across critical infrastructure and compromise data security, rather than producing stable, reliable, resilient, secure systems.[27]

These concerns and risks, and associated debates, are generally little known within wider society. As such, we are still very much at the stage of trying to understand and grapple with the consequences of producing smart cities and data-driven urbanism, and to create new policies, standards, regulations and laws that enable their benefits to be realised whilst minimising any pernicious effects.

The remainder of this report focuses on the latter two concerns and risks: ethical effects and security vulnerabilities. The report first discusses the implications of smart city technologies

and data-driven urbanism for data privacy, data protection and data security. It then sets out various strategies and policies for addressing privacy and protection concerns and tackling systemic weaknesses in data security.

The discussion somewhat inherently casts a negative light on smart city initiatives by highlighting potential privacy and security harms. Such critical analysis is important because, while the development of smart cities undoubtedly has created and will continue to create many benefits, they also raise a number of troubling issues that need to be fully considered. It is only by reflecting on and addressing these issues that we will develop smart cities that serve all parties (citizens, city authorities and companies) and deliver on their promises, while minimising their pernicious effects and addressing their weaknesses.

5. Smart cities and data privacy and protection concerns

5.1 Privacy and privacy harms

Privacy – to selectively reveal oneself to the world[28] – is a condition that many people value and it is considered a basic human right in most jurisdictions, enshrined in national and supra-national laws in various ways. How privacy is understood both as an everyday and legal concept, however, varies between cultures and contexts. In general terms, privacy debates concern acceptable practices with regards to accessing and disclosing personal and sensitive information about a person.[29] Such sensitive information can relate to a number of a personal facets and domains creating a number of inter-related privacy forms including:

- identity privacy (to protect personal and confidential data);
- bodily privacy (to protect the integrity of the physical person);
- territorial privacy (to protect personal space, objects and property);
- locational and movement privacy (to protect against the tracking of spatial behaviour);
- communications privacy (to protect against the surveillance of conversations and correspondence); and
- transactions privacy (to protect against monitoring of queries/searches, purchases, and other exchanges).[30]

As Daniel Solove[31] details, these forms of privacy can be threatened and breached through a number of what are normally understood as unacceptable practices, each of which produces a different form of harm (see Table 4).

Table 4: A taxonomy of privacy breaches and harms

Domain	Privacy breach	Description
Information collection	Surveillance	Watching, listening to, or recording of an individual's activities
	Interrogation	Various forms of questioning or probing for information
Information processing	Aggregation	The combination of various pieces of data about a person
	Identification	Linking information to particular individuals
	Insecurity	Carelessness in protecting stored information from leaks and improper access
	Secondary use	Use of information collected for one purpose for a different purpose without the data subject's consent
	Exclusion	Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors in that data

Domain	Privacy breach	Description
Information dissemination	Breach of confidentiality	Breaking a promise to keep a person's information confidential
	Disclosure	Revelation of information about a person that impacts the way others judge her character
	Exposure	Revealing another's nudity, grief, or bodily functions
	Increased accessibility	Amplifying the accessibility of information
	Blackmail	Threat to disclose personal information
	Appropriation	The use of the data subject's identity to serve the aims and interests of another
	Distortion	Dissemination of false or misleading information about individuals
Invasion	Intrusion	Invasive acts that disturb one's tranquillity or solitude
	Decisional interference	Incursion into the data subject's decisions regarding her private affairs

Source: compiled from Solove (2006)

5.2 Current approach to privacy breaches/harms

From a legal perspective, privacy breaches and harms are mostly covered under the rubric of privacy laws in the United States, whereas in the European Union it falls within the realm of data protection.[32] In both cases, the legal frameworks draw on fair information practice principles (FIPPs) that are largely constructed around personal rights regarding the generation, use, and disclosure of personal data and the obligations of data controllers with respect to these rights[33] (see Table 5). However, different emphasis is placed on these FIPPs. For example, while the OECD[34] set out eight FIPPs (see Table 5), the Federal Trade Commission (FTC) in the United States advocates just four of them (notice, consent, access and security).[35] While the EU legislation is universal across all domains (e.g., health, finance, etc.) and applies equally to all data controllers, privacy laws are mostly domain specific in the U.S.[36] Moreover, while there is common ground on how to address privacy harms, such as advocating privacy by design, enhanced data security, and access rights to check and correct data, there are differences in approach and how to implement them (in terms of obtaining consent, notification of data breaches, cross-border data flows).[37] Other jurisdictions have their own approaches.[38]

Table 5: Fair Information Practice Principles

General principle	General description	Original OECD principle and description
Notice	Individuals are informed that data are being generated and the purpose to which the data will be put.	*Purpose Specification Principle*. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Choice	Individuals have the choice to opt-in or opt-out as to whether and how their data will be used or disclosed.	*Openness Principle.* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Consent	Data are only generated and disclosed with the consent of individuals.	*Collection Limitation Principle*. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Security	Data are protected from loss, misuse, unauthorised access, disclosure, alteration and destruction.	*Security Safeguards Principle*. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
Integrity	Data are reliable, accurate, complete and current.	*Data Quality Principle*. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Access	Individuals can access, check and verify data about themselves.	*Individual Participation Principle*. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to her/him; (b) to have communicated to her/him, data relating to her/him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to her/him; (c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to her/him and, if the challenge is successful to have the data erased, rectified, completed or amended.

General principle	General description	Original OECD principle and description
Use	Data are only used for the purpose for which they are generated and individuals are informed of each change of purpose.	*Use Limitation Principle*. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified within the notice, except: with the consent of the data subject, or by the authority of law.
Accountability	The data holder is accountable for ensuring the above principles and has mechanisms in place to assure compliance.	*Accountability Principle.* A data controller should be accountable for complying with measures which give effect to the principles stated above.

Sources: Minelli *et al*. (2013); OECD (1980)

The varying legal framings and policies across jurisdictions create a fractured regulatory and compliance landscape, with different obligations existing for smart city technologies deployed within different nations (and cities depending on local laws and regulation). Nonetheless, putting this issue to one side, it is clear that across all jurisdictions smart city technologies are challenging existing legal and regulatory provisions, as well as societal norms and expectations, with respect to privacy (see Box 3).

Box 3: Privacy concerns with respect to smartphone apps

In 2015 two thirds of adults in the United States owned a smartphone (with 85% penetration amongst 18-29 year olds).[39] On average, smartphone users spent 30 hours each month using about 27 apps.[40] Many smart city technologies are accompanied by a dedicated smartphone app or third party apps utilising their APIs. The smartphone is thus a key technology through which citizens interface with and experience the smart city. As well as communicating information derived from smart city technologies, smartphones also generate significant amounts of data that, on the one hand, can feed back into smart city initiatives and, on the other, raise many privacy and security concerns.

With respect to privacy, Zang et al.,[41] note that there are four key worries with respect to smartphone apps:

First, each smartphone has unique identifiers that can be accessed and shared by apps, some of which can be captured externally via wifi or bluetooth signal. These identifiers include System ID, SIM card ID, IMEI (International Mobile Station Equipment Identity), MEID (Mobile Equipment Identifier), MAC address (Media Access Control), and UDID (Unique Device Identifier).[42] These IDs can be used to track the phone and, by association, its owner. Although the IDs are pseudonyms, they act as very clear personal markers that have a range of other information attached to them, such as phone numbers, email accounts, messaging logs, address books, social media accounts, credit card details, etc., as well as inferred information such as home and work addresses (through repeated visits and time spent at the locations).

Second, an app can request permission to access device functions, such as the camera, phone, stored media, as well personal or sensitive data such as addresses and passwords. A common worry is that many apps practice over-privileging, seeking permission to access more data and device functions than they need for their operation.[43] For example, Table 6 details the data permissions that can be sought by Android apps.

Table 6: Data permissions that can be sought by Android apps

Data type	Data permissions sought
Accounts log	email log
App Activity	name, package name, process number of activity, processed id
App Data Usage	Cache size, code size, data size, name, package name
App Install	installed at, name, package name, unknown sources enabled, version code, version name
Battery	health, level, plugged, present, scale, status, technology, temperature, voltage
Device Info	board, brand, build version, cell number, device, device type, display, fingerprint, IP, MAC address, manufacturer, model, OS platform, product, SDK code, total disk space, unknown sources enabled
GPS	accuracy, altitude, latitude, longitude, provider, speed
MMS	from number, MMS at, MMS type, service number, to number
NetData	bytes received, bytes sent, connection type, interface type
PhoneCall	call duration, called at, from number, phone call type, to number
SMS	from number, service number, SMS at, SMS type, to number
TelephonyInfo	cell tower ID, cell tower latitude, cell tower longitude, IMEI, ISO country code, local area code, MEID, mobile country code, mobile network code, network name, network type, phone type, SIM serial number, SIM state, subscriber ID
WifiConnection	BSSID, IP, linkspeed, MAC addr, network ID, RSSI, SSID
WifiNeighbors	BSSID, capabilities, frequency, level, SSID
Root Check	root status code, root status reason code, root version, sig file version
Malware Info	algorithm confidence, app list, found malware, malware SDK version, package list, reason code, service list, sigfile version

Source: Hein (2014)

Some of the data hoovered up by an app seeking these permissions, as well as device access, will be vital for an app to work. However, such wide ranging permissions clearly do not comply with the ethos of data minimisation, nor is it in the best interest of the app user. It may well be the case while permission is sought that an app does not actually access or pulldown all these data, in which case the question remains as to why excessive permissions are sought in the first place.

Third, any data collected by an app can potentially be shared with third parties, such as advertisers. In a test of 101 smartphone apps in 2011, the Wall Street Journal found that 56 transmitted the phone's unique device identifier to other companies without users' awareness or consent, 47 sent the phone's location, and 5 sent the user's personal details.[44] A similar 2015 study of 110 popular Android and iOS apps found that 73% of Android apps shared personal information such as email address with third parties, and 47% of iOS apps shared geo-coordinates and other location data with third parties.[45]

Fourth, terms and conditions with respect to apps, including privacy, can be difficult to understand given their use of legal language, length, complexity, use of vague, elastic terms like 'improving customer experience', and declarations about changing future terms unilaterally.[46] Moreover, configuring the privacy tools within the device settings is not always intuitive to non-technical users. Even more troubling is that a large number of apps do not have privacy policies that users can view and accept. For example, the European Data Protection Supervisor reported in 2014 that 39% of the most popular apps had no privacy policy.[47] Likewise, a comparison of 110 apps in 2015 found that 33% of the iOS apps and 25% of the Android apps had no privacy policies.[48] Given that there are over 1.5 million apps in the Apple App Store and 1.6 million in the Google Play Store, a very large number of apps lack privacy policies.[49]

5.3 Smart cities, privacy harms and challenges to existing regulatory approaches

Smart city technologies create a number of potential privacy harms for six inter-related reasons, each of which also raises significant challenges to existing approaches to protecting privacy. As a number of studies have highlighted, these issues are of significant concern to the general public, civil liberties organisations, legislators and regulators,[50] and have been the focus of public campaigns against smart city technologies in some cases.[51]

5.3.1 Intensifies datafication

Smart city technologies capture data relating to all forms of privacy and radically expand the volume, range and granularity of the data being generated about people and places.[52] Importantly, the capture and circulation of these data are:

1. indiscriminate and exhaustive (involve all individuals, objects, transactions, etc.);
2. distributed (occur across multiple devices, services and places);
3. platform independent (data flows easily across platforms, services, and devices);
4. continuous (data are generated on a routine and automated basis).[53]

Further, tasks that were previously unmonitored or potentially captured only through a disciplinary gaze, such as what television programmes one watches or the settings of a home heating thermostat or journeys across a city, are now routinely tracked and traced through smart technologies (see Box 4). The result is the production of detailed longitudinal datasets. These datasets are easily shared and can be conjoined to other datasets to extract additional insights. Since the data are organised and stored in digital databases, they are highly suited to examination using data analytics.[54]

Such datafication has four effects with respect to privacy. First, people are now subject to much greater levels of intensified scrutiny and modes of surveillance and dataveillance than ever before[55], with smart city technologies providing deeply personal pictures of individual lives, especially when datasets are combined together.[56] Second, the pervasiveness of digitally-mediated transactions and surveillance, plus the increasing use of unique identifiers and PII to access services (e.g., names, usernames, passwords, account numbers, addresses, emails, phone details, credit card numbers, smart card ID, license plates, faces), means that it is all but impossible to live everyday lives without leaving digital footprints (traces we leave ourselves) and shadows (traces captured about us).[57] Third, the mass recording, organising, storing and sharing of big data about a phenomenon changes the uses to which such data can be put, both for good and for ill.[58] Fourth, such data enables a lot of inference beyond the data generated to reveal insights that have never been disclosed.

Box 4: Location and movement tracking

Up until relatively recently tracking the movement of individuals was a slow, labour-intensive, partial and difficult process.[59] The only way to track the location and movements of an individual were to follow them in person and to quiz those with whom they interacted. As a result, people's movement was undocumented unless there was a specific reason to focus on them through the deployment of costly resources. Even if a person was tracked, the records tended to be partial, bulky, difficult to cross-tabulate, aggregate and analyse, and expensive to store.

A range of smart technologies has transformed geo-location tracking to a situation where the monitoring of location is pervasive, continuous, automatic and relatively cheap, it is straightforward to process and store data, and easy to build up travel profiles and histories. For example:

- Many cities are saturated with remote controllable digital CCTV cameras that can zoom, move and track individual pedestrians. In addition, large parts of the road network and the movement of vehicles are surveyed by traffic, red-light, congestion and toll cameras. Analysis and interpretation of CCTV footage is increasingly aided by facial, gait and automatic number plate recognition (ANPR) using machine vision algorithms. Several police forces in cities in the UK have rolled out CCTV facial recognition programmes,[60] as have cities in the U.S., including New York and Chicago (each with over 24,000 cameras) and San Diego (who are also using smartphones with facial recognition installed).[61] ANPR cameras are installed in many cities for monitoring traffic flow, but also for administrating traffic violations such as the non-payment of road tolls and congestion charging. There are an estimated 8,300 ANPR cameras across the UK capturing 30 million number plates each day.[62]
- Smartphones continuously communicate their location to telecommunications providers, either through the cell masts they connect to, or the sending of GPS coordinates, or their connections to wifi hotspots. Likewise, smartphone apps can access and transfer such information and also

share them to third parties. With respect to the latter, Leszczynski's analysis of the data generated by The Wall Street Journal in 2011[63] details that 25 out 50 iPhone apps, and 21 of 50 Android apps transmitted location data to a third party other than the app developer[64]. These data are used to target advertising and utilised by data brokers to create user profiles. For example, 'Verizon have a product called Precision Market Insights that let businesses track cell phone users in particular locations.'[65]

- In a number of cities, sensor networks have been deployed across street infrastructure such as bins and lampposts to capture and track phone identifiers such as MAC addresses. In London, Renew installed such sensors on 200 bins, capturing in a single week in 2014 identifiers from 4,009,676 devices and tracking these as they moved from bin to bin.[66] The company reported that they could measure the proximity, speed, and manufacturer of a device and track the stores individuals visited, how long they stayed there, and how loyal customers are to particular shops, using the information to show contextual adverts on LCD screens installed on the bins.[67]The same technology is also used within malls and shops to track shoppers, sometimes linking with CCTV to capture basic demographic information such as age and gender.[68]
- Similarly, some cities have installed a wifi mesh, either to provide public wifi or to create a privileged emergency response and relief communication system in the event of an urban disaster or for general surveillance. In the case of public wifi, the IDs of the devices which access the network are captured and can be tracked between wifi points. In the case of an emergency/police mesh, access might not be granted to the network; however each network access point can capture the device IDs, device type, apps installed, as well as the locational history.[69] Such a wifi mesh, with 160 nodes, was installed by the Seattle Police Department in 2013.[70] The locational history of previous wifi access points is revealed because a wifi-enabled device broadcasts the name of every network it has connected to previously in order to try and find one it can connect to automatically. Beyond a wifi-mesh, anyone with a wi-fi adapter in monitor mode and a packet capture utility can capture such data.[71]
- Many buildings use smart card tracking, with unique identifiers installed either through barcodes or embedded RFID chips. Cards are used for access control to different parts of the building and to register attendance, but can also be used as an electronic purse to pay for items within the facility. Smart card tracking is becoming increasingly common in many schools to track and trace student movements, activities and food consumption.[72] Smart cards are also used to access and pay for public transport, such as the Leapcard in Dublin or the Oyster Card in London. Each reading of the card adds to the database of movement within a campus or across a city.
- New vehicles are routinely fitted with GPS that enables the on-board computers to track location, movement, and speed. These devices can be passive and store data locally to be downloaded for analysis at a later point, or be active, communicating in real-time via cellular or satellite networks to another device or data centre. Active GPS tracking is commonly used in fleet management to track goods vehicles, public transport and hire cars, or to monitor cars on a payment plan to ensure that it can be traced and recovered in cases of default, or in private cars as a means of theft recovery. Moreover, cars are increasingly being fitted with unique ID transponders that are used for the automated operation and payment of road tolls and car parking. Again, each use of the transponder is logged, creating a movement data trail, though with a larger spatial and temporal granularity (at selected locations).
- Selected populations — such as people on probation, prisoners on home leave, people with dementia, children — are being electronically tagged to enable tracking. Typically this is done using a GPS-enabled bracelet that periodically transmits location and status information via a wireless telephone network to a monitoring system. In other cases, it is possible to install tracker apps onto a phone (of say children) so the phone location can be tracked, or to buy a family tracking service from telecoms providers.[73]

- There are also many other staging points where we might leave an occasional trace of our movement and activities, such as using ATMs, or using a credit card in a store, or checking a book out of a library. Another form of staging point is the use of the Internet, such as browsing or sending email, where the IP address of the computer reveals the approximate location from which it is connected. Typically this does not have a fine spatial resolution (mile to city or region scale), but does show sizable shifts of location between places. Another set of staging points can be revealed from the geotagging (using the device GPS) and time/date stamping of photos and social media posted on the internet and recorded in their associated metadata. This has more spatial resolution than IP addresses and is also accompanied with other contextual information such as the content of the photo/post.[74]
- Location and movement can also be voluntarily shared by individuals through online calenders, most of which are private but nonetheless stored in the cloud with a service provider, and some of which are shared openly or with colleagues.

As these examples demonstrate, those companies and agencies who run these technologies possess a vast quantity of highly detailed spatial behaviour data from which lots of other insights can be inferred (such as mode of travel, activity, and lifestyle). Moreover, these data can be accessed by the police and security forces through warrants or more surreptitiously, and can be shared with third party partners for commercial purposes. The consequence is that individuals are no longer lost in the crowd, but rather they are being tracked and traced at different scales of spatial and temporal resolution, and are increasingly becoming open to geo-targeted profiling for advertising and social sorting.

5.3.2 Deepens inferencing and creates predictive privacy harms

Predictive modelling using urban big data can generate inferences about an individual that are not directly encoded in a database but constitute what many would consider to be PII and which produce 'predictive privacy harms.'[75] For example, co-proximity and co-movement with others can be used to infer political, social, and/or religious affiliation, potentially revealing membership of particular groups.[76] Likewise, the volunteered information of a few people on social media can unlock the same undisclosed information about the many through social network analysis and pattern recognition, creating what Barocas and Nissenbaum[77] term the 'the tyranny of the minority'. It has been calculated that knowing the sexual orientation of just twenty percent of social media users will enable the orientation of all other users to be inferred with a high degree of accuracy.[78]

Similarly, tracking data that reveals a person regularly frequents gay bars, leading to the inference that the person is likely to gay, would be considered by many as personal and sensitive data, especially in places that are still intolerant of gay relationships. If any inference of sexual orientation produced by a predictive model was shared, for example through advertising sent to the family home or via social media on a shared computer, then it could cause personal harm. Yet, as no data about sexuality has been directly collected, Crawford and Schultz[79] note that any company or organisation making such inferences has 'no obligation under current privacy regimes to give notice to, or gather consent from its customers in the same way that direct collection protocols require.' Moreover, these inferences can generate inaccurate characterization that then stick to and precede an individual. This is a particular issue in predictive policing and anticipatory governance, where

the profiling of both people and places can reinforce or create stigma and harm, particularly when the underlying data or models are poor.

5.3.3 Weak anonymization and enables re-identification

One of the key strategies for ensuring individual privacy is anonymization, either through the use of pseudonyms, aggregation or other strategies. The generation of big data and new computational techniques, however, can make the re-identification of data relatively straightforward in many cases. Pseudonyms, in particular, simply mean that a unique tag is used to identify a person in place of a name. As such, the tag is anonymous in so far that code is used to identify an individual. However, the code is persistent and distinguishable from others and recognisable on an on-going basis, meaning it can be tracked over time and space and used to create detailed individual profiles.[80] As such, it is no different from other persistent pseudonym identifiers such as social security numbers and in effect constitutes PII.[81] The term 'anonymous identifier', as used by some companies,[82] is thus somewhat of an oxymoron, especially when the identifier is directly linked to an account with known personal details (e.g., name, address, credit card number). Even if the person is not immediately identifiable, the persistence of the pseudonym enables data controllers to act on that data and shape how they interact with individuals. As such, pseudonyms 'enable holders of large datasets to act on individuals, under the cover of anonymity, in precisely the ways anonymity has long promised to defend against' and they place no inherent limits on an institution's ability to track and trace the same person in subsequent encounters.[83]

Further, inference and the linking of a pseudonym to other accounts and transactions means it can potentially be re-identified. Indeed, it is clear that it is possible to reverse engineer anonymisation strategies by combing and combining datasets[84] unless the data are fully de-identified. De-identification requires both direct identifiers and quasi-identifiers (those highly correlated with unique identifiers) to be carefully removed.[85] The extent to which this is happening before data are shared with third parties is highly doubtful. Moreover, there are some companies that specialise in re-identification of data across big data datasets.[86] Such is the concern that the New Zealand Privacy Commissioner and the New Zealand Data Futures Forum have advocated legal protections against re-identification.[87]

5.3.4 Opacity and automation creates obfuscation and reduces control

The emerging big data landscape is complex and fragmented. Various smart city technologies are composed of multiple interacting systems run by a number of corporate and state actors.[88] For example, the app ecosystem (including app developers, app owners, app stores, operating systems, mobile carriers, devices) is conjoined to the data source ecosystem (e.g., an API of real-time bus data), which similarly consists of a range of hardware, software and organisations. Data are thus passed between synergistic and interoperable 'devices, platforms, services, applications, and analytics engines'[89] and shared with third parties. Moreover, across this maze-like assemblage they can be 'leaked, intercepted, transmitted, disclosed, dis/assembled across data streams, and repurposed' in ways that are difficult to track and untangle.[90] The result is that it can be very difficult to

know precisely the life of data and how they are used and transformed into new derived data.[91] Nor is it easy to understand the tangled set of roles (as data processors and controllers) and obligations between actors and where responsibilities and liabilities reside.[92]

Adding to the opacity of systems is that the generating, processing, sharing and acting on data are increasingly becoming automated. Automation of smart city technologies exists at three levels:[93]

- **human-in-the-loop:** systems identify and select profiles and targets, but the system will only respond with a human command (e.g., facial recognition matches being manually assessed before proceeding);
- **human-on-the-loop:** systems identify and select profiles and targets, and can act on them but under the oversight of a human operator who can over-ride the system (e.g., SCADA systems, or intelligent transport control rooms); and
- **human-out-of-the-loop:** the system identifies and selects profiles and targets and acts on them without any human input or interaction (e.g., automatically: using ANPR to detect congestion charge breaches and issue fines; adding suspects to no-fly lists based on data mining; conducting trades on the stock market; purging voters from registration lists).[94]

Human-out-of-the-loop implements a form of automated management in which decisions are automated, automatic and autonomous in nature.[95] Within such automated systems, the rules for acting on data and making decisions is black-boxed. Yet it is well known that programmers routinely, if unintentionally, change the substance of rules when translating them into computer code, despite not having the delegated authority to do so.[96] Moreover, weak algorithms and dirty or error-prone data can generate high rates of false positives and baseless decision making. The result is that the 'transparency, accuracy, and political accountability of administrative rulemaking are lost', policy and law are inadvertently distorted, and critical procedural safeguards are potentially dismantled.[97] This makes external oversight and scrutiny difficult, especially in cases where the system adjudicates in secret or lacks audit trails.[98] These automated systems can be Kafkaesque; for example, no-fly lists where people are not informed as to why they have been placed on the list, yet nor can they argue against the decision.[99]

Opacity and automation undermine the FIPPs at the heart of privacy regulation in a number of respects; making it difficult for individuals to seek access to verify, query, correct or delete data, or to even know who to ask; to know how data collected about them is used; to assess how fair any actions taken upon the data are; and to hold data controllers to account.[100] Automated systems makes notice and consent all but impossible, since 'the public has no opportunity to review new rules embedded in closed source code' and 'individuals lack notice of the new rules that will bind them.'[101] Moreover, meaningful judicial review is impaired and technological due process is lacking.[102]

5.3.5 Data are being shared and repurposed and used in unpredictable and unexpected ways

One of the key features of the data revolution is the wholesale erosion of data minimisation principles; that is, the undermining of purpose specification and use limitation principles that mean that data should only be generated to perform a particular task, are only retained as long as they are needed for that task, and are only used to perform a particular task.[103] These principles are largely antithetical to the rationale of big data and the functioning of data markets which seek to generate and hoard large volumes of data to extract additional value.[104] The solution pursued by many companies is to repackage data by de-identifying them (using pseudonyms or aggregation) or creating derived data, with only the original dataset being subjected to data minimisation. The repackaged data can then be sold on and repurposed in a plethora of ways that have little to do with the original reason for data generation and without the need to give notice or consent to those that the data concerns.[105]

Such data practices are now common, enabling the rapid growth of data brokers (sometimes called data aggregators or consolidators or resellers) which capture, gather together and repackage data into privately held data infrastructures for rent (for one time use or use under licensing conditions) or re-sale, along with data analysis and profiles.[106] Trading data and data services is a multi-billion dollar industry consisting of a diverse eco-system of different types of data brokers ranging from very large consolidators to a range of specialist companies focused on particular markets or services. In 2014, Angwin identified 212 data brokers operating in the US that consolidated and traded data about people, only 92 of which allowed opt-outs (65 of which required handing over additional data to secure the opt-out), and 58 companies that were in the mobile location tracking business, only 11 of which offered opt-outs.[107] Data derived from smart city technologies and associated apps circulate within these data markets.

The data and services these companies offer are used to perform a wide variety of tasks for which the data were never intended, including to predictively profile, socially sort, behaviourally nudge, and regulate, control and govern individuals and the various systems and infrastructures with which they interact.[108] Smart city technologies and the data they generate thus have significant direct and in-direct impact on people's everyday lives. These impacts can be both positive and negative, but in both cases raise numerous questions about privacy and privacy harms.

For example, a key product of data brokers are predictive profiles of individuals as to their likely tastes and what goods and services they are likely to buy, or their likely value or worth to a business, or their credit risk and how likely they are to pay a certain price or be able to meet re-payments. These profiles can be used to socially sort and redline populations, selecting out certain categories to receive a preferential status and marginalising and excluding others. In other words, the profiles can be used to make decisions as to whether a person might be approved for a loan, or a tenancy or mortgage, or a job, or even what price they might pay in a store.[109] This has led to concerns that a form of 'data determinism' is

being deployed in which individuals are not simply profiled and judged on the basis of what they have done, but on a prediction of what they might do in the future.[110]

Data determinism is most clearly expressed in forms of anticipatory governance, such as that used in predictive policing, where predictive analytics are used to assess likely future behaviours or events and to direct appropriate action. A number of US police forces are now using predictive analytics to anticipate the location of future crimes and to direct police officers to increase patrols in those areas. For example, the Chicago police force produce both general area profiling to identify hotspots and guide patrols, and more specific profiling that identifies individuals within those hotspots.[111] It achieves the latter using arrest records, phone records, social media and other data to construct the social networks of those arrested to identify who in their network is most likely to commit a crime in the future, designating them 'pre-criminals' and visiting them to let them know that they have been flagged in their system as a potential threat.[112] In such cases, a person's data shadow does more than follow them; it precedes them.

In all these cases, few of those whose data has fed into creating predictive profiles imagined that their data were going to be repurposed to social sort or regulate or control them, or nudge them towards certain behaviours. As such, data repurposing can break what is considered compatible forms of data re-use and the reasonable expectations of data subjects.[113]

5.3.6 Notice and consent is an empty exercise or is absent

Notice and consent – considered the cornerstone of data and privacy protection – are significantly weakened within smart city technologies. Given issues of datafication, inference, repurposing and opacity, notice and consent can become an empty exercise or it is absent.

As noted above, individuals interact with a number of smart city technologies on a daily basis, each of which is generating data about them. Given the volume and diversity of these interactions, it is simply too onerous for individuals to police their privacy across dozens of entities, to weigh up the costs and benefits of agreeing to terms and conditions without knowing how the data might be used now and in the future, and to assess the cumulative and holistic effects of their data being merged with other datasets.[114] Even if someone wanted to proactively manage their data privacy across all these systems and apps, they would be faced with long, complex legal documents[115] that in practice are non-negotiable – one either consents or is denied the service.[116]

As a result, providing notice and seeking consent become an empty exercise as: '(1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decision-making difficulties.'[117] Consent thus often consists of individuals unwittingly signing away rights without realising

the extent or consequences of their actions.[118] The consequence is 'privacy policies often serve more as liability disclaimers for businesses than as assurances of privacy for consumers.'[119] Moreover, from a regulatory perspective, the question becomes 'Did the data handler follow the right procedures to obtain consent?' rather than 'Did the data subject consent?'[120]

In other cases, notice and consent are absent, either unimplemented or difficult to achieve in practice. As detailed in Box 3, between a quarter and a third of all smartphone apps lack a privacy policy and do not seek consent. Notice and consent for downstream activities such as data mining and repurposing are often covered by catch-all disclaimers, along with the right to unilaterally change terms and conditions without notice, effectively disenfranchising individuals of choice, control and the accountability of service providers. In the case of some smart city technologies, there is little mechanism to seek notice and consent, but also little choice in being surveilled. For example, CCTV, ANPR and MAC address tracking, and sensing by the Internet of Things all take place with no attempt at consent and often with little notification (though there may be notice in the form of information signs in the area being surveilled, or on related websites). Moreover, there is no ability to opt-out[121] other than to avoid the area, which is unreasonable and unrealistic. As such, there is no sense in which a person can selectively reveal themselves; instead they must always reveal themselves.[122] Moreover, if a person is unaware that data about them is being generated, then it is all but impossible to discover and query the purposes to which those data are being put.[123]

6. Smart cities and data security concerns

There are two key security concerns with respect to smart cities. The first is the security of smart city technologies and infrastructures and the extent to which they are vulnerable to being hacked via a cyberattack. The second is the security of the data generated, stored and shared across such technologies and infrastructures. The latter is directly related to the former as improper access to data is often achieved via security weaknesses in a system's components, architecture and operation. In this sense, information security (data protection) has converged with operational security (making sure things work reliably and with integrity).[124]

6.1 Operational security and cyberattack

Smart city solutions utilise complex, networked assemblages of digital technologies and ICT infrastructure to manage various city systems and services. Any device that relies on software to function is vulnerable to being hacked. If a device is networked, then the number of potential entry points multiples across the network, and the hack can be performed remotely.[125] Once a single device is compromised, then the whole assemblage becomes vulnerable to cyberattacks that seek to 'alter, disrupt, deceive, degrade or destroy computer systems and networks or the information and/or programs resident in or transiting these systems or networks.'[126] There are three forms of cyberattack: availability attacks that seek to close a system down or deny service use; confidentiality attacks that seek to extract information and monitor activity; and integrity attacks that seek to enter a system to alter information and settings (such as changing settings so that components exceed normal performance, erasing critical software, planting malware and viruses).[127] The vulnerability of systems is exacerbated by a number of issues including weak security and encryption; the use of insecure legacy systems and poor maintenance; large and complex attack surfaces and interdependencies; cascade effects; and human error and disgruntled (ex) employees (see Box 5). The result is that the process of making city systems and infrastructures 'smart' has also made them vulnerable to a suite of cyber-threats.[128]

Box 5: Types of security vulnerabilities

Weak security and encryption

All software-enabled devices are vulnerable to exploits and attacks. A Carnegie Mellon University report details that, on average, there are 30 bugs or possible exploits for every 1000 lines of code.[129] In complex systems with millions of lines of code that produces thousands of potential zero-day exploits[130] for viruses, malware and hacks. The most common means of protection is to use encryption, usernames/passwords, firewalls, virus and malware checkers, security certificates, and security patch updates to close exploits to try and limit the ability of attackers to access software and data. However, the extent to which this suite of protections is used varies across technologies and vendors. Research by cybersecurity specialists has discovered that many smart city systems have been constructed with no or minimal security[131] and city governments and vendors are deploying them without undertaking cybersecurity testing[132] (see Box 6). In the case of some Internet of Things deployments, it can be difficult to ensure end-to-end security because most sensors and low-powered devices on the market do not have sufficient computing power to support an encrypted link.[133] Where encryption is used, security issues can arise due to poor key generation, fixed keys, shared keys, and leaked keys.[134]

The use of insecure legacy systems and poor maintenance

A related issue is that many smart city technologies are layered onto much older infrastructure that relies on software and technology created 20 or 30 years ago, which has not been upgraded for some time, nor can they be migrated to newer, more secure systems.[135] These technologies can create inherent vulnerabilities to newer systems by providing forever-day exploits.[136] Some would go as far to say that any device or system that is not regularly patched and upgraded should be considered part of the 'darknet'; that is, treated as if it is compromised.[137] Even in the case of newer technologies, it can be difficult to test and rollout patches onto critical operational systems that need to always be on.[138]

Large and complex attack surfaces and interdependencies

Smart city systems are typically large, complex and diverse, with many interdependencies with other systems and many stakeholders involved. It can be difficult, therefore, to know what and how all the components are exposed, to measure and mitigate risks, and to ensure end-to-end security.[139] Even if independent systems are secure, linking them to other systems will open them to risk with the level of security only guaranteed by the weakest link.[140] Moreover, the interdependencies between technologies and systems mean that they are harder to maintain and upgrade.[141]

Cascade effects

The interdependencies between smart city technologies and systems have the potential to create cascade effects, wherein 'highly interconnected entities rapidly transmit adverse consequences to each other.'[142] For example, an attack on an energy system could cascade into an urban operating system that then cascades into the other systems such as traffic management, emergency services, water services, etc. Indeed, this is one of the key security and resilience risks of an urban operating system.[143] A successful cyberattack on the electricity grid has huge cascade effects as it underpins so many activities such as powering homes, work, other infrastructure, and so on.[144]

Human error and disgruntled (ex)employees

Technical exploits can be significantly aided by human error, for example, employees opening phishing emails and installing viruses or malware, or inserting infected datasticks into computers.[145] Errors can also occur in relation to how data are released. For example, in 2014 a freedom of information request resulted in the release of data on 173 million journeys undertaken by New York taxis in one year. The data were incorrectly anonymised and relatively easy to decode, revealing the driver IDs, pickup and drop-off times, and GPS routes taken for all cab journeys.[146] In other cases, security is not installed or is installed incorrectly, or manufacturer installed codes are not changed or system security is not kept up-to-date.[147] In some cases, systems can be deliberately sabotaged by disgruntled present and ex-employees.[148]

Cyberattacks on critical infrastructure have become a significant issue in recent years. Dell Security reported that there were 675,186 cyberattacks against industrial control systems in January 2014.[149] Electricity grid utilities in the US report being under near constant cyberattack, with one utility recording that it was the target of approximately 10,000 cyberattacks each month.[150] The Israel Electric Corp. reports that its servers register about 6,000 unique computer attacks every second, with other critical infrastructure also under continuous cyberattack.[151] Many of these cyberattacks are relatively inconsequential, such as probes and address scans, and are unsuccessful, while a small number are much more significant and involve a security breach. In a 2014 study of 599 utility, oil and gas, energy and manufacturing companies, nearly 70 percent reported at least one security breach that

led to the loss of confidential information or disruption of operations in the previous 12 months;[152] 78 percent expected a successful attack on their ICS (industrial control systems) or SCADA (supervisory control and data acquisition) systems in the next two years.[153] In 2012, 23 gas pipeline companies were hacked and source code and blueprints to facilities stolen.[154] Between 2010 and 2014, the US Department of Energy (that oversees the US power grid, nuclear arsenal, and national labs) documented 1,131 cyberattacks, of which 159 were successful.[155] In 53 cases, these attacks were 'root compromises', meaning that the attackers gained administrative privileges to computer systems, stealing various kinds of personnel and operational information.[156] These cyberattacks target every type of smart city solution and particular system components (see Box 6). Somewhat worryingly, most businesses are not aware that they have been hacked.[157] One study found that the average time for detection was 210 days and in 92 percent of cases, the discovery was via an angry customer, law enforcement agency, or a contractor.[158]

Table 7: IoT Attack Surface Areas

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Ecosystem Access Control	Implicit trust between components Enrolment security Decommissioning system Lost access procedures	**Local Data Storage**	Unencrypted data Data encrypted with discovered keys Lack of data integrity checks
Device Memory	Cleartext usernames Cleartext passwords Third-party credentials Encryption keys	**Third-party Backend APIs**	Unencrypted PII sent Encrypted PII sent Device information leaked Location leaked
Device Physical Interfaces	Firmware extraction User CLI Admin CLI Privilege escalation Reset to insecure state Removal of storage media	**Vendor Backend APIs**	Inherent trust of cloud or mobile application Weak authentication Weak access controls Injection attacks
Device Web Interface	SQL injection Cross-site scripting Cross-site Request Forgery Username enumeration Weak passwords Account lockout Known default credentials	**Update Mechanism**	Update sent without encryption Updates not signed Update location writable Update verification Malicious update Missing update mechanism No manual update mechanism

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Device Firmware	Hardcoded credentials Sensitive information disclosure Sensitive URL disclosure Encryption keys Firmware version display and/or last update date	**Ecosystem Communication**	Health checks Heartbeats Ecosystem commands Deprovisioning Pushing updates
Device Network Services	Information disclosure User CLI Administrative CLI Injection Denial of Service Unencrypted Services Poorly implemented encryption Test/Development Services Buffer Overflow UPnP Vulnerable UDP Services DoS	**Mobile Application**	Implicitly trusted by device or cloud Username enumeration Account lockout Known default credentials Weak passwords Insecure data storage Transport encryption Insecure password recovery mechanism Two-factor authentication
Administrative Interface	SQL injection Cross-site scripting Cross-site Request Forgery Username enumeration Weak passwords Account lockout Known default credentials Security/encryption options Logging options Two-factor authentication Inability to wipe device	**Cloud Web Interface**	SQL injection Cross-site scripting Cross-site Request Forgery Username enumeration Weak passwords Account lockout Known default credentials Transport encryption Insecure password recovery mechanism Two-factor authentication
Network Traffic	LAN LAN to Internet Short range Non-standard		

Source: OWASP[159]

Cyberattacks can be performed by hostile nations, terrorist groups, cyber-criminals, hacker collectives, and individual hackers. Former FBI director, Robert Mueller, details that 108 nations have cyberattack units, targeting critical infrastructure and industrial secrets.[160] The majority of attacks are presently being repulsed using cybersecurity tools, or their effects have been disruptive or damaging but not critical for the long term delivery of services.[161] Indeed, it needs to be recognised that to date, successful cyberattacks on cities are still relatively rare and when they have occurred their effects generally last no more than a few hours or involve the theft of data rather than creating life threatening situations. That said, it is clear that there is a cybersecurity arms race underway between attackers and defenders, and that more severe disruption of critical infrastructure has been avoided through the threat of mutually assured destruction between nations.[162] This is not to suggest that smart city initiatives should be avoided, but rather that the cybersecurity challenges of creating secure smart cities are taken seriously. As Box 6 details it is likely that cyberattacks will increase over time; they will become more sophisticated and have the potential to cause significant disruption to city services and the wider economy and society.[163]

Box 6: Cybersecurity and smart city technologies

All forms of smart city technologies are vulnerable to cyberattack. There are a number of weak points – including SCADA systems, the sensors and microcontrollers of the Internet of Things, and communication networks and telecommunication switches – which facilitate the kinds of security vulnerabilities set out in Box 5.

SCADA systems

Various forms of urban infrastructure, including the electricity grid, water supply, and traffic control, rely on SCADA (supervisory control and data acquisition) systems that are used to control functions and flow.[164] These systems measure how an infrastructure is performing in real-time and enable either automated or human operator interventions to change settings. SCADA systems can be traced back to the 1920s, but were extensively rolled out in the 1980s.[165] As a consequence, many deployments are quite dated. Many have been found to operate with their original security codes. In some cases, while the infrastructure is relatively secure, the communications network is vulnerable.[166] A number of SCADA systems, as detailed below, have been compromised, with hackers altering how the infrastructure performs, or causing a denial-of-service, or have stolen data. Probably the most infamous SCADA hack was the 2009 Stuxnet attack on Iran's uranium enrichment plant in which the system was infected by malware that destroyed a number of centrifuges by running them beyond their design specifications.[167] By 2010, over 90,000 Stuxnet infections were reported in 115 countries.[168]

Cameras

Cities are full of a plethora of CCTV cameras; some owned and controlled privately, others by public authorities and police services. The security of these cameras is highly variable, with some lacking encryption or usernames and passwords, and others open to infection by malware and firmware modification.[169] Accessing a camera provides a means to spy on individuals, such as viewing home presence or using a bank ATM camera to monitor the digits being pressed. Demonstrating the scale of the issue, one website provides access to the feeds of thousands of unsecured or poorly secured cameras (uses admin passwords) from 152 countries.[170] Cameras can also be turned off, with some lacking the function to be restarted remotely.[171]

Internet of Things

The Internet of Things refers to the connecting together of machine-readable, uniquely identifiable objects across the Internet. Some objects are passive and can simply be scanned or sensed (such as smart cards with embedded RFID chips used to access buildings and transport systems). Others are more active and include microcontrollers and actuators. All kinds of objects that used to be dumb, such as fridges, thermostats and lights, are now becoming networked and smart, generating information about their use and becoming controllable from a distance. Moreover, sensors can be embedded into the urban fabric and throughout critical infrastructures to produce data concerning 'location, proximity, velocity, temperature, flow, acceleration, sound, vision, force, load, torque, pressure, and interactions.'[172] Sensors and microcontrollers are hackable as they often have little effective security, encryption, or privacy protocols in place.[173]

Communication networks and telecommunication switches

The Internet of Things are linked together via a number of communications technologies and protocols such as 4G LTE (Long Term Evolution), GSM (Global System for Mobile communication), CDMA (Code Division Multiple Access), WiFi, bluetooth, RFID (Radio-Frequency Identification), NFC (Near-Field Communication), ZigBee (open wireless standard), and Z-Wave (wireless communication). Each of the modes of networking and transferring data are known to have security issues that enable data to be intercepted and provide access to devices. Likewise, telecommunication switches that link together the local and long distance Internet infrastructure are known to have vulnerabilities including manufacturer and operator back-door security access and access codes that are infrequently updated.[174]

Electricity grid and smart meters

The generation, transmission, and distribution of electricity are monitored and controlled using SCADA systems.[175] In addition, the electricity grid consists of a range of other networked devices. In the case of the US energy grid, over 70 percent of components are over 25 years old, including many SCADA systems.[176] Given the potential cascade effects of shutting down the electricity grid, it has been a key point of cyberattack. As smart grids and smart meters are installed, the number of potential access points to grid networks increases enormously.[177] Smart meters themselves can be hacked with low-cost tools and readily available software to alter proof of consumption or to steal energy from other users.[178]

Building management systems

Building management systems are often considered an aspect of property services rather than IT services and cybersecurity is not a key issue in purchase or operation.[179] The consequence is weakly protected systems, often still configured with manufacturer codes. Moreover manufacturers often do not have processes in place for responding to vulnerabilities or a notification process to inform customers about security threats.[180] The vulnerabilities of building management systems pose two main threats.[181] The first is that if they are hacked building operations could be disrupted and safety risks created. The second is that they provide a potential route for breaking into enterprise business systems and critical company data if they share the same network.[182]

Transport management systems and vehicles

There have been a number of cyberattacks on transport management systems in recent years, as well as proof-of-concept demonstrations of possible attacks. For example, a cyberattack on a key toll road in Haifa, Israel, closed it for eight hours causing major traffic disruption.[183] A research team from the University of Michigan managed to hack and manipulate more than a thousand traffic lights in one city using a laptop and wireless radio.[184] Likewise, IOActive Labs have hacked traffic

control sensors widely used around the world and altered traffic light sequencing and interactive speed and road signs.[185] A teenager in Lodz, Poland, managed to hack the city tram switches, causing four trams to derail and injuring a number of passengers.[186] In the US, air traffic control systems have been hacked, FAA servers seized, the personal information of 58,000 workers stolen, and malicious code installed on air traffic networks.[187] Vehicles themselves are also open to being hacked given that a new car contains up to 200 sensors connected to around 40 electronic control units and can connect to wireless networks.[188]

6.2 Security of data

Data-driven urbanism produces, processes, stores, and shares vast quantities of data and derived data and information. Much of these data are sensitive in nature. While some data can be made open and shared freely, as with data released through urban dashboards (see Box 2), most is considered private and needs to be held securely and kept protected. Given the value of data to cybercriminals for identity theft and blackmail, to companies for gaining industrial secrets, and nation states for security and cyberwar, they are much sought after.

News concerning major data breaches or national surveillance programmes is, at present, an almost weekly occurrence, and it is clear that data security has become a significant weak point of networked endeavours. Informationisbeautiful.net provides details on 185 data breaches, including the source and size of the breach.[189] Over 100 of the incidents involve over 1 million customer accounts breached (with over 20 involving >100m records), with sensitive data stolen including names, addresses, social security numbers, credit card details, administrative and patient records. The Ponemon Institute reported in 2014, based on a survey of 567 executives of US businesses, that 43 percent of firms had experienced a data breach in the previous year involving the loss of more than 1000 records.[190] The average cost to the company for each lost or stolen record was estimated to be $201, incurred through direct compensation to customers and credit card companies, class-action lawsuits by customers, shareholders and regulators, loss in share price, and investigation costs and new security measures.[191] For example, the hack of Sony PlayStation in June 2011 resulted in the loss of 77 million accounts including credit card details, names, addresses, date of birth, and log-in credentials, and cost the company more than $1 billion in lost business, law suits, and outside contractors.[192] The consequence for the individuals to whom the data refers is identity theft, leading to criminal activity that is attributed to them, and the stress and effort involved in trying to clear one's name. 12.6 million Americans were reportedly the victims of identity theft in 2012 at the collective loss of $21 billion.[193]

Data breaches occur for all the reasons detailed in Box 5 and have become more common because the lines of attack have grown as more and more systems and infrastructures become networked. And yet, it is apparent that in too many cases, security is an afterthought, applied after a system has been developed and prototyped, and that companies are often more interested in convenience, minimisation of downtime, and marginal efficiency than security and compliance.[194] In the Ponemon Institute study, 27 percent of companies did not have a data breach response plan or team in place and 46 percent did not have privacy and data protection awareness training for employees and other stakeholders who have access to sensitive personal information.[195] Of those

companies with a plan only 30 percent said their organisation was effective or very effective in developing and executing it.[196] In a separate Unisys and Ponemon Institute survey of critical infrastructure companies, only 28 percent ranked security as one of the top five strategic priorities for their organisation.[197] Moreover, 58 percent reported that they only partially or never vetted contractors, vendors and other third-parties for high security standards.[198] Only 17 percent of companies described their cybersecurity as mature, and only 6 percent provided cyber-security training for all employees.[199]

With respect to smart city technologies specifically, it is clear that many vendors have little or no experience in embedding security features into their products and many systems possess significant vulnerabilities[200] (see Box 6). These vendors can impede security research by limiting access to their systems for testing, enabling them to continue to release unsecured products without oversight or accountability.[201] As troubling, most cities have limited cybersecurity budgets and resources and do not have cyberattack threat models prepared, mitigation strategies developed, and response plans in place, nor do they have designated cybersecurity personnel and leadership (in the form of CIOs and CTOs[202]) and CERTs (Computer Emergency Response Teams), meaning they lack an effective, coordinated reaction if their systems are hacked.[203] Cybersecurity expertise is usually limited to a handful of personnel and training across the entire workforce is limited (increasing the likelihood of human error issues). Any cybersecurity plans cities do possess are often siloed with respect to particular systems and departments, so that cross-function assessment and response is lacking.[204] Indeed, it is often not clear who is responsible when a smart city is hacked or crashes,[205] especially when there are multiple systems and stakeholders involved. It is thus important that smart city designers and planners and city leaders start to take more seriously the threat of cyberattack and the 'normal accidents'[206] that threaten operational and data security.

7. Addressing data privacy and security concerns with respect to the smart city

It is clear from the discussion so far that there are a number of data privacy, protection and security concerns and challenges created through the rollout of smart city technologies. Addressing these issues is no simple task, both politically and pragmatically. Indeed, there are two distinct levels to the debate. The first examines more general normative questions concerning the ethics and politics of mass surveillance enabled by smart city technologies and the use of urban big data in predictive profiling, social sorting, anticipatory governance and the management of city populations, infrastructures and services. The second level is more concerned with how to best implement data privacy, protection and security given present legislation and expected norms.

These two levels are strongly related given that a position held with respect to the first directly influences the position taken with respect to the second. For example, a position that accepts the need for mass surveillance and the erosion of privacy will advocate for different interventions than a position that is much more committed to individual privacy and personal autonomy. At present, the debate over the mass surveillance of society largely hinges on two inherent trade-offs: between privacy and national security; and between privacy and economic growth.[207]

In the first case, surveillance is cast as a choice between creating safer societies or defending personal autonomy. On the one side, trust is traded for control, and all citizens are treated as potential threats without warranted suspicion for the greater good of national security. On the other side, privacy is seen as an 'indispensable structural feature of liberal democratic political systems'[208] and is foundational to informed and reflective citizenship and to freedom of expression.[209] The danger of mass surveillance for the latter is the loss of core societal values of freedom and liberty to be replaced by highly controlled and authoritarian societies.

In the second case, the mass generation of data about customers is cast as a choice between creating new products, markets, jobs and wealth or individual and collective rights. On the one side, it is argued that data privacy and security should not hinder innovation and the extraction of economic value of individual data, or impede customer experience.[210] Without new innovations, it is suggested, the economy will stagnate and society will suffer. On the other side, it is contended that it is possible to extract value from big data and create new products without infringing on privacy and aggressively micro-targeting and profiling individuals.[211]

Within both trade-off cases, privacy is often positioned as mutually exclusive from national security and economic development. Privacy, the argument goes, is dead or dying,[212] even if there are those who do not fully realise it yet; it has been sacrificed for the supposed greater good. Further, those in favour of the mass generation of data resort to arguments such as 'if you have nothing to hide, you have nothing to fear', or 'if you do not like how we operate, do not use our service.' As critics note, the first assertion conflates privacy with the

concealment of suspicious behaviour, as opposed to personal autonomy, freedom of expression, and the selective choice to reveal oneself.[213] The second is entirely impractical and unreasonable given that email, online banking and shopping, credit cards, smartphones, social media, and so on, are the tools of modern life, necessary for a career and social life.[214] Opting out is not a viable choice. Indeed, with respect to many smart city technologies, opting out is not even an option.

While the privacy debate can sometimes be framed in quite black and white terms, the reality is that it is really full of greys. Privacy is not dead, though it is certainly under attack and in transition, and privacy is not mutually exclusive to national security and economic development. Privacy does still remain a key value for individuals, even if they find it increasingly difficult to manage and protect in practice.[215] It is still protected through legislative and regulatory instruments, even if these presently struggle with the unfolding data revolution. Moreover, people and companies want their data to remain secure. The real issue is the balance between privacy and other interests and ensuring the right tools are in place to maintain the balance desired.

The following practical and pragmatic solutions to data privacy, protection and security concerns and harms related to smart cities are framed within a position that does not see privacy and security/development as mutually exclusive and which still values the FIPPs set out in Table 5. Following Angwin, it attempts to find a middle way between 'those who ask us to hand over all our data and 'get over it,' and those who suggest that we throw our body on the tracks in front of the speeding train that is our data economy.'[216] In this sense, the aim has been to identify solutions that enable the rollout of smart city technologies, but to do so in a way that is not prejudicial to citizens; that actively work to minimise privacy harms, minimises data breaches, and tackles cybersecurity issues; and that work across the entire life-cycle (from procurement to decommissioning) and the span of a whole system ecology (all its stakeholders and components).

The approach advocated is multi-pronged as there is no single solution for all of the concerns detailed above. Rather a suite of solutions is needed, some of which are market driven, some more technical in nature, others more governance and management orientated, and some more policy, regulatory and legally focused. Together these will enact what has been termed 'smart privacy' – a broad arsenal of protections including: 'privacy by design; law, regulation and independent oversight; accountability and transparency; market forces; education and awareness; audit and control; data security; and fair information practices.'[217] Importantly, the approaches advocated are not heavy handed in nature, seeking mutual consensus, collaboration and to be enabling rather than restrictive. Moreover, they should be relatively inexpensive to implement as they are principally about changing practices and redeploying existing resources and staff more effectively.

7.1 Market solutions

Market solutions to privacy and security issues generally fall into two camps. The first is a contention that the market will adapt to self-regulate privacy and data security in line with societal demand for fear of losing customers and market share.[218] The main problem with

this argument is that it assumes that companies will actively self-regulate as opposed to resist and block change, that individuals have the freedom and choice to move their custom, and that any abuses of privacy will be enough to enact such behaviour. Some companies are effectively quasi-monopolies in particular domains, with consumers having few other choices. Further, while some companies will be ethical and conscientious in seeking to ensure data privacy and security, market regulation does not solve the issue of vendors who wilfully abuse privacy rights or are negligent in their data security practices. Moreover, individuals often do not understand the implications of terms and conditions associated with different products and systems, nor their privacy rights, and often do not act in their own self-interest.

The evidence suggests that companies generally only change privacy policies to favour their own interests or when under duress and to comply with legislation and regulation[219]. Indeed, in many cases, privacy policy changes are to update terms and conditions to cover more extensive data generation and data uses and to further limit liabilities. Here, companies have used the emergence of big data to undermine and work around FIPP expectations. Moreover, there has been active lobbying to reduce data protection provisions designed to address many of the issues detailed in Section 5.3. With respect to data security, companies will often prioritise convenience, service continuity, cost savings and marginal efficiency over security.[220] As such, while undoubtedly self-regulation has a role to play in protecting data privacy, it cannot be the only solution, with a need for governance mechanisms and legal and regulatory tools and oversight to ensure compliance.

The second market solution is for companies to see consumer privacy and data security as a competitive advantage, developing privacy and security protocols and tools that will attract consumers away from other vendors.[221] For example, companies developing products that have limited tracking or profiling, or end-to-end encryption. While welcome, the concern is that privacy and security might become a two-tiered system, available for a fee rather than as a right. In addition, as data breaches and privacy scandals continue to tarnish the development of inter-networked products and services, the cybersecurity industry itself will continue to grow to provide enhanced privacy and security tools and technologies. Such technical solutions will be aimed at individuals so that they can more effectively manage their privacy, and companies and public authorities so that they can better protect their operational security, data resources, and the privacy of their customers and clients.

7.2 Technology solutions

As noted, too many smart city technologies have large attack surfaces that have a number of vulnerabilities, especially in systems that contain legacy components using old software which has not been regularly patched. Technology solutions to data privacy and security seek to use technical fixes and products to effectively manage systems and tackle risks. At one level, this consists of implementing best practice solutions in building and maintaining secure smart city infrastructures and systems.

This includes:

- strong, end-to-end encryption;
- strong passwords and access controls;
- firewalls;
- up-to-date virus and malware checkers;
- security certificates;
- audit trails;
- isolating trusted resources from non-trusted;
- disabling unnecessary functionality;
- ensuring that there are no weak links between components;
- isolating components where possible from a network;
- implementing fail safe and manual overrides on all systems;
- ensuring full backup of data and recovery mechanisms; and
- automatically installing security patch updates on all components, including firmware, software, communications, and interfaces.[222]

The aim is to reduce the attack surface as much as possible and to make the surface that is visible as robust and resilient as possible.

At another, complementary level, the approach has been to develop a suite of Privacy Enhancing Technologies (PETs) that seek to provide individuals with tools to protect their PII and dictate how PII should be handled by different services. PETs have been defined by the European Commission as 'a coherent system of information and communication technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data without losing the functionality of the information system.'[223] In effect, PETs seek to minimise data generation, increase individual control of PII, choose the degree of online anonymity and linkability of data, track the use of their data, gain meaningful consent, and facilitate legal rights of data inspection, correction and deletion.[224] PETs include relatively simple tools such as ad blockers, cookie blockers and removers, malware detection and interception, site blocking, encryption tools, and services to opt-out of databases held by data brokers.[225] In general, these kinds of PETs are aimed at protecting PII on websites and smartphones and managing how data are handled by data brokers and have limited application with respect to many smart city technologies which generate data about people in a different way (through cameras, smart card readers, sensors, etc.). Other approaches such as statistical disclosure control (SDC), private information retrieval (PIR), and privacy-preserving data mining (PPDM) are aimed at protecting confidentiality in data analysis and the release of public datasets, database retrieval, and data mining.[226]

7.3. Policy, regulatory and legal solutions

While market-driven and technological solutions will have a number of positive effects, how they are administered is framed by the wider policy, regulatory and legal landscape. It is clear that the present regulatory and legal tools with respect to privacy and security are not fit for purpose in the age of urban big data and algorithmic governance and need revision. It is not the intention of this report to prescribe new legal and regulatory provisions for smart cities and privacy and security more broadly. Indeed, this is the focus of a number of initiatives already at the EU and national level. Instead, it advocates the use of four pragmatic policy approaches which seek to address privacy and security harms and concerns.

7.3.1 Fair information practice principles (FIPPs)

FIPPs are the core principles underlying the generation, use and disclosure of personal data and the obligations of data controllers. A number of the principles set out in Table 5 have been eroded since FIPPs were first published by the OECD in 1980, in part due to the active lobbying of the data industry to limit their liabilities and responsibilities and extend the value they can extract from data, and in part due to the rise of big data and the fundamental changes in the nature of data. The fact that FIPPs are now difficult to apply in practice and are routinely being circumvented has highlighted the need to revisit and revise them. This need has been recognised in the EU and a number of countries, such as the US, Canada and New Zealand.[227] For example, The White House (2012) sets out a revised set of FIPPs in its 'Consumer Privacy Bill of Rights' for the big data age.

- *Individual Control*: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- *Transparency*: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- *Respect for Context*: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- *Security*: Consumers have a right to secure and responsible handling of personal data.
- *Access and Accuracy*: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- *Focused Collection*: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- *Accountability*: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

These updated FIPPs extend those officially advocated by the FTC, and widen the scope of shared principles, expanding consumer control over information at issue and how the data are used.[228] The FTC and EU have also focused recently on re-emphasising the need for data

minimisation.[229] While this reworking of FIPPs is important, critics argue that they do not go far enough in protecting against many of the issues detailed in Section 5.3, especially predictive privacy harms arising from inferencing, data being shared, repurposed and used in unpredictable and unexpected ways, and notice and consent being an empty exercise or absent.[230] Nonetheless, revised FIPPs fit for the big data age would provide an important core set of underlying principles for the deployment of privacy and security-led smart city technologies.

7.3.2 Privacy by design

One means by which FIPPs can become much more central to the development of smart city technologies is through the adoption of privacy by design. While regulatory and legislative compliance seeks to ensure that vendors and cities fulfil their obligations with respect to privacy by correctly and fairly handling the data they generate and manage, privacy by design proposes that privacy is the default mode of operation[231]. Rather than collecting data, assuming they are all available for use (unless the individual does not consent, which effectively means they are denied the service), all data remain private unless the consumer explicitly says otherwise. In other words, privacy is hardwired into the design specifications and usage of information technology, business practices, physical environments, and infrastructure of systems and apps through the adoption of seven foundational principles (see Table 8)[232]. Because these are principles and not a set of prescribed methods, they provide latitude for different modes of implementation. The approach is positioned as a 'positive-sum' (rather than zero-sum) solution that does not rely on trade-offs between privacy rights and other issues such as security or economic development, but rather seeks to maximise both[233]. The use of privacy by design has been advocated by the EU, FTC and a number of national information/data protection commissioners.

Table 8: The principles of privacy by design

Principle	Description
Proactive not reactive; preventative not remedial	IT systems should seek to anticipate privacy concerns rather than seeking to resolve privacy infractions once they have incurred
Privacy as the default setting	Privacy is automatically protected and does not require action on behalf of an individual
Privacy embedded into design	Privacy protections are core features of the design and architecture of IT systems and is not a bolt-on feature
Full functionality - positive-sum, not zero-sum	All legitimate interests and objectives are accommodated, rather than there being trade-offs between privacy and other considerations such as security
End-to-end security - full lifecycle protection	Privacy is embedded into the system from ingestion to disposal
Visibility and transparency - keep it open	Component parts and operations are visible and transparent to users and providers alike and are subject to independent verification
Respect for user privacy - keep it user-centric	A system should be built around, protect the interests, and empower individuals

Source: Cavoukian (2009)

7.3.3. Security by design

Complementary to privacy by design is security by design. Likewise, a proactive and preventative rather than reactive and remedial approach is taken to security, seeking to build it into systems from the outset rather than layering it on afterwards. This requires security risk assessment to be a fundamental part of the design process and security measures to be rigorously tested before the product is launched,[234] including a test pilot phase within a living lab environment that includes testing the security of a product when deployed as part of a wider network of technologies (to ensure end-to-end security). It also means having in place an on-going commitment to cybersecurity, including a mechanism to monitor products throughout their life cycle, a process of supporting and patching them over time, and a procedure for notifying customers when security risks are identified. A key commitment of security by design is for end-to-end encryption and strong access controls, including forcing adopters to change default passwords,[235] and to only keep data essential for the task being performed and transferring data in aggregated form where possible.[236]

7.3.4. Education and training

Revised FIPPs, privacy-by-design and security-by-design provide practical policy interventions aimed at shaping how privacy and security are tackled by those developing smart city technologies. There is a need for these to be complemented with education and training policies aimed at shaping users' understanding of how these technologies work and their privacy and security practices, and to inform developers of their obligations and best practices. To this end, four national education and training programmes are advocated.

The first is a general education programme directed at the public that sets out the privacy and security implications of various smart city technologies and the practical steps they can take to protect themselves against privacy and security harms. This would be complemented by an educational programme aimed at school children that warns them about the data being generated about them and informs them about how to best to manage their data privacy and security. The third is a training programme aimed at local authority staff who are involved in the development of smart city policy formulation, the procurement of smart city technologies, or the rollout and running of smart city initiatives. This programme would include a general overview of data protection obligations, but also a grounding in how to evaluate privacy and security concerns and implement privacy/security impact assessments. The fourth is a training programme aimed at technology companies, and in particular start-ups and SMEs who might not have the in-house capacity for privacy and security expertise, to set out their obligations and best practices that might give them a competitive advantage. In the Irish case this training might be delivered through the fifteen Enterprise Ireland technology centres, or via the Start-Up Commissioner or agencies such as The Digital Hub and NDRC (National Digital Research Centre) that run support programmes for start-ups, or university sponsored tech incubators and innovation hubs.

7.4 Governance and management solutions

A critical component of well-run city systems and infrastructures is their governance and management structures and processes. Governance provides the framework through which

strategic direction is deliberated and set, and regulation and oversight administered. Management consists of leading and driving forward initiatives and stewarding the day-to-day running of services. Together they frame the rollout and maintenance of city systems and infrastructures and ensure they work as intended, fulfil their ambitions and strategic intent, and stay within legal and regulatory parameters.

Putting in place strong principle-led governance and management is therefore a prerequisite for creating a smart city that seeks to maximise benefits while minimising harms. And yet, to date, there are very few documented cases of such governance and management structures being constituted. Instead, smart city initiatives have been procured and developed with little coordinated consideration of privacy and security harms and slotted into existing city management in an ad hoc fashion with minimal strategic oversight.

Given the potential harms and the associated costs that can arise, and the potential benefits at stake, this piecemeal approach needs to be discontinued to be replaced with a more strategic, coordinated approach that consists of interventions at three levels: vision and strategy (smart city advisory board); oversight of delivery and compliance (smart city governance, ethics and security oversight committee); and day-to-day delivery (core privacy/security team and computer emergency response team). This approach recognises that there is a need for collaboration between experts in different domains to ensure sharing of knowledge and shared learning.

7.4.1. Smart city advisory boards

A smart city advisory board is a high-level forum for the strategic visioning of the composition, form and ambition of its smart city plan and the principles underpinning the deployment and management of smart city initiatives. The aim is to create a broad consensus as to:

- how the evolving smart city should unfold;
- how it will align and shape the wider city development plan;
- the ethos and ethics underlying the smart city agenda;
- the necessary governance and management structures; and
- the sourcing of necessary resources and finances, and the means to evaluate rollout and success.

From these deliberations, smart city policies will be formulated, including the adoption of an ethical framework that sets out clearly the FIPPs adopted. Over time, the role of the advisory board will evolve to consider whether the smart city programme is on-track, is fulfilling its ambition and is meeting its principles, as well as whether its governance and management is functioning well.

The advisory board should consist of a panel of key stakeholders, including representatives of local and regional government, other relevant state agencies, regulatory bodies, private companies and their representative bodies, third sector groups, and community organisations. Members should have relevant knowledge and expertise of smart city technologies and related concerns and harms, urban planning and development, city governance and management, and local community issues. Given that the intent is strategic and agenda setting, rather than direct oversight or management, the advisory board would ideally meet two or three times a year.

As yet, there seem to be few examples of documented, formally constituted smart city advisory boards.[237] The Smart London Board[238] is one case, drawing together experts from academia, business and entrepreneurship to guide the development of London's smart city strategy. One of its first deliverables was the Smart London Plan.[239] Seattle does not have smart city advisory board, but has established a privacy advisory board that sets out a set of principles with respect to smart city technologies and the wider use of digital technologies by city authorities (see Box 7). Seattle's approach is instructive because it does reaffirm the use of FIPPs and seeks to establish an ethical framework to guide data privacy and security with respect to smart city technologies.

Box 7: Seattle Privacy Advisory Committee

In response to the privacy implications of smart city technologies and a number of criticisms of the city's data practices, Seattle has established a Privacy Advisory Committee (PAC) to assess the ways in which the city authorities generate, store and use data, and to consider issues such as confidentiality, anonymity, archival procedures, deletion, sharing and publishing as open data, and the ability to conduct forensic internal audits.[240]

The PAC initiative is led by the city's Department of Information Technology and its Chief Technology Officer and consists of various public and private stakeholders,[241] including the city police, fire, lighting, transportation, information technology and law departments, Seattle Public Library, academics and industry leaders.

The PAC is tasked with setting out a set of principles with respect to data privacy and developing a privacy toolkit. This toolkit includes annual privacy and security classes to educate city departments and workers on the latest privacy practices and access compliance, and implementing a Privacy Impact Assessment (PIA) protocol for evaluating the risks for new forms of data collection.[242] The PIAs will be made available on a publicly accessible website. The aim is to continue to evolve the city's privacy policies and practices as new technologies and legal obligations dictate.[243]

The PAC has published a set of basic privacy principles.[244] In essence, these principles simply confirm that the city is following FIPPs and its already existing legal obligations. They are complemented by a much more detailed privacy statement[245] that sets out the city policy on privacy issues.

Critics would like the PAC to have a wider membership and be supplemented with an executive-level Chief Privacy Officer and a core team of dedicated staff who have responsibility for ensuring that the privacy principles and toolkit are implemented, and constitute a single point of contact for all city departments with regards to privacy queries from the public.[246] Nonetheless, the PAC and the city's approach to privacy is a useful approach and instructive for other cities.

7.4.2. Smart city governance, ethics and security oversight committee

A smart city governance, ethics and security oversight committee is much more operationally focused than an advisory boards. Their intent is to:

- oversee and audit the work of the privacy/security team;
- advise on the work priorities and programme;
- certify that the city's smart city strategies are being implemented and meeting targets and that they conform to legal and regulatory requirements;
- ensure that response and mitigation plans and processes are in place; and
- ensure there is clear communication to public concerning how the smart city is being realised and how data are being generated, used, stored and shared.[247]

With respect to the latter, Transport for London (TfL) is a model organisation setting out very clear data use and retention policies (see Box 8).

A task for the governance, ethics and security oversight committee would be to certify smart city ethics/security assessments in line with adopted FIPPs. For each smart city initiative, these assessments would determine:

- what data are to be generated;
- how the data are to be processed and analysed and what derived data can be produced;

- the ownership and access to the data and derived data;
- the conjoining of data with other datasets;
- how the data might be leveraged and repurposed;
- the sharing and transfer of data to third parties;
- the presentation/publication of information derived from the data;
- the security of data and how the data are stored; and
- the plans for dealing with breaches and hacks.

During the procurement process, the extent to which the proposed solutions meet these parameters would influence the evaluation of tenders. For smart city initiatives that are already deployed, the assessments would be used to evaluate how closely they match the desired parameters and to develop a roadmap for achieving future compliance with the city's desired formulation. This is important because it is incumbent on city authorities to broker privacy and security arrangements on behalf of citizens, given that notice and consent are all but impossible in many cases. In this way, the city gets to shape the privacy and data protection landscape through its contracting procedures and parameters. In all cases of potential and existing smart city initiatives, all vendors should be asked for full privacy and security documentation and service level agreements should include on-time patching and 24/7 incident response.[248]

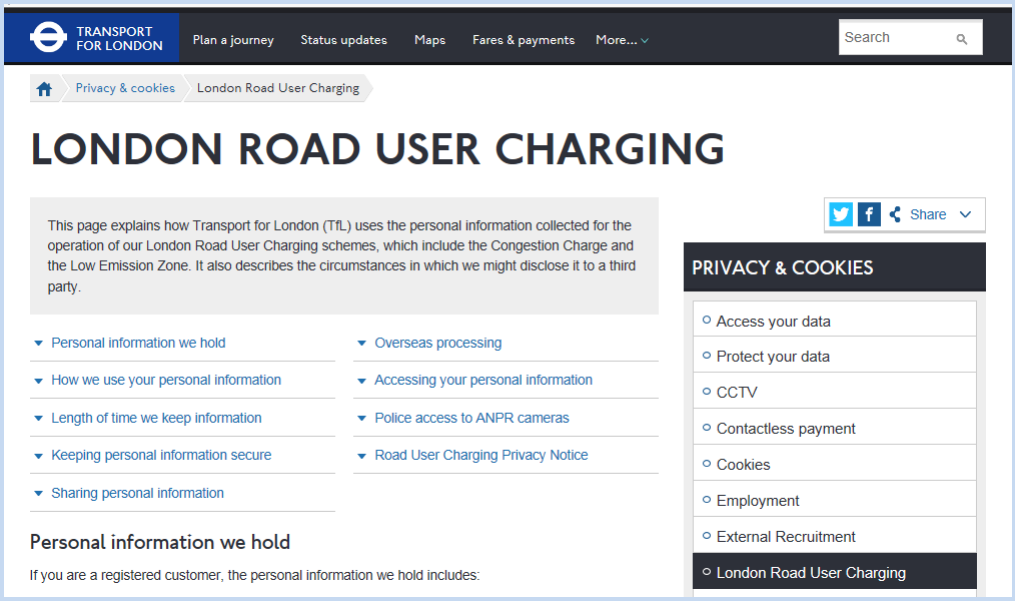
A smart city governance, ethics and security oversight committee should meet four to six times a year and be composed of a small number of expert external members (three to four) and a small group of key city officials, including any CIOs, CTOs or CDOs[249] and the head of the privacy/security core team. Governance, risk and oversight boards are a statutory feature of public sector bodies in many jurisdictions, and the smart city version will need to be accommodated within the existing governance structure.

Box 8: Transparent data policy: Transport for London (TfL)

Transport for London (TfL) is the local government body responsible for public transport in London, with responsibility for running and overseeing over-ground and underground rail, buses, water services, cycling, taxis and private hire, and dial-a-ride services.[250]

As a large organisation coordinating travel for millions of passengers daily, TfL generates and manages a massive amount of data from a diverse set of sources including: websites and smartphone apps, CCTV in stations and on trains and buses, contactless and credit card payments, Oyster cards (inc. photo in some cases), congestion charging, bike use, lost luggage requests, taxi licensing, its 25,000+ employees, job applicants, etc.

TfL has adopted a transparent approach to data privacy and data protection policies, which are published on their website.[251] These policies are short, clear and unambiguous, written in plain English that avoids dense legal language.



For each type of data TfL detail: what personal information they hold, why they collect that information, how they use the information; the length of time they keep it before deleting (varies from 24 hours to 7 years, depending on type and purpose[252]), how they secure it, how they share it, if any of the data are processed overseas, how someone can access the data held about them, any relevant privacy notices. Where necessary links are provided to specific pieces of external policy or regulation/law.

7.4.3. Core privacy/security team

The core privacy/security team is responsible for the day-to-day delivery of the city's strategy and policies, and undertaking the work within the framework dictated by the governance, ethics and security oversight committee. Its work would include:

- liaising with the city departments and companies administering smart city initiatives;
- undertaking threat and risk modelling;
- testing the security of smart city technologies (rather than simply trusting vendor reassurances);
- conducting smart city ethics/security assessments (including privacy impact assessments);
- coordinating staff training on privacy and security issues; and
- communicating smart city policies to the public.

As a routine part of their work, the core privacy/security team should consult with cybersecurity vendors to stay up-to-date on potential threats and solutions.[253] In addition, the team should create a formal channel for security feedback and ethical disclosure, enabling bugs and security weaknesses to be reported by members of the public and companies.[254] Ethics and security assessments should be carried out as early as possible, for example in the scoping and procurement phases of technological adoption, to ensure the

solutions developed conform to expectations. The team would consist of a number of dedicated staff.

7.4.4. City Computer Emergency Response Teams (CERTs)

CERTs consist of a team of key personnel, drawn from the core privacy/security team, IT services, smart city initiatives and emergency services, that spring into action when a smart city technology experiences a cybersecurity incident and is hacked and records stolen or the system disrupted or terminated.[255] In this sense, they are similar to other emergency response teams that tackle other city events. CERTs prepare detailed plans of action and accountability/responsibility in the case of different types of incidents.[256] These plans are reviewed and updated on a regular basis as new technologies are rolled out. In the context of Ireland, given the size of the cities and institutional capacities it might be that local authority and city cybersecurity needs will be covered solely by the new National Cyber Security Centre (NCSC) which hosts the national/governmental Computer Security Incident Response Team (CSIRT-IE)[257]. In addition, the Irish Reporting and Information Security Service, an independent non-for-profit company, also provides a CERT service[258].

8. Conclusion

The danger with a report focused on data privacy, data protection and data security in the context of smart cities is that it becomes overly focused on the negative concerns and harms. These concerns can then segue into a highly cautious approach which stifles innovation and rollout that means the potential benefits of smart cities are not realised. However, while the concerns relating to smart cities are significant, we need to remain mindful of their potential benefits in producing more efficient, productive, sustainable, resilient, transparent, fair and equitable cities.

The challenge is to acknowledge that there are a set of very real issues and concerns that do need to be addressed, and to find and adopt solutions to these that also enable the benefits of smart city technologies to be gained. In other words, there is a need to chart a path that is neither so luddite that no developments can occur, nor too boosterist or scare-mongering that fundamental values of privacy, liberty and freedom are sacrificed for a data economy or a surveillant, securitised state.

Ignoring or deliberately avoiding smart city technologies is not a viable approach; nor is developing smart cities that create a range of harms and reinforce power imbalances. Rather we need to create a particular kind of smart city that has a set of ethical principles and values at its heart. Such a balanced approach is not straightforward to conceive or implement given the diverse set of stakeholders and vested interests at work in the smart city space.

This report provides one vision of a balanced strategy to data privacy, data protection and data security in the context of smart cities and advocates a multi-pronged approach that blends together market, technical, governance and management, and policy, regulatory and legal solutions. Together these solutions seek to promote fairness and equity, protect citizens and cities from harms, and enable the benefits of smart cities and urban big data to be realised. Moreover, they do so using an approach that is not heavy handed in nature and is relatively inexpensive to implement.

The next step is for the good practice developed so far to be built on, and the solutions suggested to be advanced further conceptually, deployed in practice, and evaluated, with iterative learning applied. What cannot be allowed to happen is a continuation of the ad hoc and arbitrary approach taken to date and data privacy, data protection and data security harms to multiply unchecked. We need to be smart in our approach to smart cities.

Acknowledgements

The research in this report was funded by the Department of Taoiseach and builds on initial research undertaken as part of European Research Council funded 'The Programmable City' project (ERC-2012-AdG-323636). The author would like to thank: Dara Murphy TD, Minister of State at the Departments of the Taoiseach, Justice & Equality, and Foreign Affairs & Trade with Special Responsibility for European Affairs and Data Protection; the members of the Government Data Forum; staff of the Data Protection Unit, Department of the Taoiseach; Claudio Coletta, Leighton Evans, Liam Heaphy, Jim Merricks White and Sung-Yueh Perng of the Programmable City project, Maynooth University; Mark Boyle of the National Institute for Regional and Spatial Analysis at Maynooth University; Claire Davis from Cork Smart Gateway; Jamie Cudden and Pauline Riordan from Smart Dublin; and Simon Marvin, University of Sheffield for their help in sourcing material and advice.

The image in Box 1 is from http://ipprio.rio.rj.gov.br/centro-de-operacoes-rio-usa-mapas-feitos-pelo-ipp/ and is reproduced under fair usage for comment, scholarship and research in the public good. The image in Box 7 is a screen grab of Seattle privacy program website - http://www.seattle.gov/information-technology/privacy-program - and is reproduced under fair usage for comment, scholarship and research in the public good. The image in Box 8 is a screen grab of the TfL website - https://tfl.gov.uk/corporate/privacy-and-cookies/road-user-charging - and is reproduced under fair usage for comment, scholarship and research in the public good.

Endnotes

[1] Kitchin (2014a)

[2] Townsend (2013)

[3] Kitchin (2014a; 2015a)

[4] Schaffers *et al*. (2011); Batty *et al*. (2012)

[5] Caragliu *et al*. (2009)

[6] Townsend (2013)

[7] Kitchin (2015b)

[8] Giffinger *et al*. (2007); Hollands (2008); Cohen, B. (2012); Townsend (2013)

[9] Kitchin (2015c)

[10] See www.dublindashboard.ie/pages/DublinApps

[11] Kitchin (2015a)

[12] Kitchin (2014a)

[13] KItchin (2014b)

[14] See Kitchin and McArdle (2015)

[15] Singer (2012)

[16] centrodeoperacoes.rio/institucional

[17] Singer (2012)

[18] centrodeoperacoes.rio/institucional

[19] Kitchin (2014a; 2015c)

[20] Block and van Assche (2010); Kitchin *et al*. (2015)

[21] Greenfield (2013); Mattern (2013); Morozov (2013)

[22] Greenfield (2013)

[23] Kitchin (2014a), Kitchin *et al*. (2015)

[24] Hill (2013); Shelton *et al*. (2015)

[25] Datta (2015)

[26] Graham (2005); Dodge and Kitchin (2005); Kitchin and Dodge (2011); Elwood and Leszczynski (2013); Vanolo (2014)

[27] Kitchin and Dodge (2011); Townsend (2013); Cerrudo (2015)

[28] Cypherpunk Manifesto, cited in Angwin (2014)

[29] Elwood and Leszczynski (2011)

[30] Martínez-Ballesté *et al*. (2013); Santucci (2013)

[31] Solove (2006)

[32] Minelli *et al.* (2013); Fuster and Scherrer (2015)

[33] Solove (2013)

[34] OECD (1980)

[35] FTC (2000)

[36] Barocas and Nissenbaum (2014)

[37] Santucci (2013)

[38] See dlapiperdataprotection.com/#handbook/world-map-section for an overview of data protection laws around the world.

[39] Pew Research Center (2015)

[40] Nielson (2014)

[41] Zang *et al*. (2015)

[42] Zang *et al*. (2015)

[43] Zang *et al*. (2015)

[44] Efrati *et al.* (2011)

[45] Zang *et al*. (2015)

[46] European Data Protection Supervisor (2014: 34)

[47] European Data Protection Supervisor (2014)

[48] Graves (2015)

[49] Statista (2015) cited in Zang et al. (2015)

[50] Rainie and Anderson (2014); Article 29 Data Protection Working Party (2014); Crump and Harwood (2014)

[51] Seattle Privacy Coalition (n.d.) https://www.seattleprivacy.org/; Murphy (2015)

[52] Crawford and Schultz (2014); Kitchin (2014b)

[53] Leszczynski (forthcoming); Kitchin (2014b)

[54] Strandberg (2014)

[55] Lyon (2014)

[56] Ramirez (2013); Murphy (2015)

[57] Dodge and Kitchin (2005)

[58] Strandberg (2014)

[59] Angwin (2014); Kitchin (2015d)

[60] Graham (2011); Gardham (2015)

[61] Wellman (2015)

[62] Weaver (2015)

[63] blogs.wsj.com/wtk-mobile/

[64] Of these, 19 of the iPhone apps and 13 of the Android apps did not require locational data as a functional requirement. Half the iPhone and a third of the Android apps did not request consent for passing on the locational data.

[65] Angwin (2014: 8). Through Precision Market Insights, Verizon sells data 'about its cell phone users' "age range, gender and zip codes for where they live, work, shop and more" as well as information about mobile-device habits, including URL visits, app downloads and usage, browsing trends and more' (Angwin 2014: 145).

[66] Vincent (2014)

[67] Vincent (2014)

[68] Kopytoff (2013); Henry (2014)

[69] Hamm (2013), cited in Leszczynski (forthcoming)

[70] Hamm (2013), cited in Leszczynski (forthcoming)

[71] Gallagher (2014)

[72] Goodman (2015)

[73] Tarantola (2014)

[74] Such data can be used in interesting ways such as tackling cyber-bullying by revealing the location of posters (Riotta 2015).

[75] Barocas and Nissenbaum (2014); Crawford and Schultz (2014)

[76] Soltani and Gellman (2013); Leszczynski (forthcoming)

[77] Barocas and Nissenbaum (2014: 61)

[78] Mislove et al. (2010) cited in Barocas and Nissenbaum (2014)

[79] Crawford and Schultz (2014: 98)

[80] Barocas and Nissenbaum (2014)

[81] Article 29 Data Protection Working Party (2014)

[82] e.g., Google, https://www.google.com/policies/privacy/key-terms/

[83] Barocas and Nissenbaum (2014: 55)

[84] Narayanan and Shmatikov (2010); de Montjoye *et al*. (2013); Ducklin (2015)

[85] Cavoukian and Castro (2014)

[86] Minelli *et al.* (2013); Goodman (2015)

[87] O'Neill (2014); New Zealand Data Futures Forum (2014)

[88] Article 29 Data Protection Working Party (2014); Fuster and Scherrer (2015); Barocas and Nissenbaum (2014)

[89] Leszczynski (forthcoming)

[90] Leszczynski (forthcoming)

[91] Fuster and Scherrer (2015)

[92] Barocas and Nissenbaum (2014)

[93] Human Rights Watch (2012); Citron and Pasquale (2014)

[94] Citron (2007-2008); Pasquale (2015)

[95] Dodge and Kitchin (2007)

[96] Citron (2007-2008)

[97] Citron (2007-2008: 1254)

[98] Citron (2007-2008)

[99] Angwin (2014)

[100] Barocas and Nissenbaum (2014); Fuster and Scherrer (2015); Strandberg (2014)

[101] Citron (2007-2008: 1291)

[102] Citron (2007-2008)

[103] Tene and Polonetsky (2012). For example, Article 6(1)(b) of the EU Data Protection Directive provides that personal data must be 'collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes' (European Data Protection Supervisor 2014)

[104] Tene and Polonetsky (2012); Andrejevic (2013)

[105] Solove (2007)

[106] CIPPIC (2006); Kitchin (2014b)

[107] Angwin (2014: 151, 161). She also notes that in 2013 Krux Digital had identified 328 separate companies tracking visitors to the top fifty content websites (p. 167).

[108] Kitchin (2014a, b)

[109] Graham (2005); Angwin (2014); Kitchin (2014b).

[110] Ramirez (2013)

[111] Stroud (2014)

[112] Stroud (2014)

[113] Article 29 Data Protection Working Party (2014); European Data Protection Supervisor (2014)

[114] Solove (2013)

[115] This is despite the fact that within the EU, the Directive on Unfair Contract Terms upholds the notion of 'good faith' and 'requires contract terms to be drafted in plain and intelligible language, with any doubt about the meaning of a term to be interpreted in favour of the consumer'; European Data Protection Supervisor (2014: 24).

[116] European Data Protection Supervisor (2014: 34)

[117] Solove (2013: 1888)

[118] Rubinstein (2013)

[119] Tene and Polonetsky (2012)

[120] Strandberg (2014: 31)

[121] Crump and Harwood (2014)

[122] Cypherpunk Manifesto, cited in Angwin (2014)

[123] Article 29 Data Protection Working Party (2014); European Data Protection Supervisor (2014)

[124] Brenner (2014)

[125] Nanni (2013)

[126] Owens *et al*. (2009)

[127] Singer and Friedman (2014)

[128] Singh and Pelton (2013); Townsend (2013); Peters (2015)

[129] Goodman (2015)

[130] As yet unknown security vulnerabilities

[131] Using the Shodan search engine – https://www.shodan.io/ – it is possible to find all kinds of devices and systems connected to the internet – from baby monitors and home heating systems to traffic control systems and command-and-control centres for nuclear power plants – many of which have been found to have little to no security (such as no username/passwords, or using defaults, e.g., 'admin', '1234'). www.wired.com/2013/07/shodan-search-engine/; money.cnn.com/2013/04/08/technology/security/shodan/index.html

[132] Cerrudo (2015)

[133] Article 29 Data Protection Working Party (2014)

[134] Cerrudo (2015)

[135] Elena Kvochko cited in Rainie *et al*. (2014); Cerrudo (2015)

[136] Whereas vendors and security firms might quickly produce a patch for zero-day exploits, forever-day exploits are holes in legacy systems that vendors no longer support and which will therefore never be patched; Townsend (2013).

[137] Jerry Michalski cited in Rainie *et al*. (2014)

[138] Cerrudo (2015)

[139] Article 29 Data Protection Working Party (2014); Cerrudo (2015); Durbin (2015)

[140] Sarma (2015)

[141] Sarma (2015)

[142] Durbin (2015); Peters (2015)

[143] Linking several systems together has the benefit of enabling a 'system of systems' approach to managing city services and infrastructures. However, it also undoes the mitigation effects of using a siloed approach (Little 2002; Simon Marvin, talk at Cyber Salon, University of Manchester, January 15th).

[144] As evidenced by the 2003 blackout in north eastern United States which bought the region to a standstill (US Department of Energy 2004).

[145] Singer and Friedman (2014)

[146] Pandurangan (2014); In a different case, Experian sold personal data relating to 200 million US citizens, including names, addresses and social security numbers to an ID theft ring in Vietnam (Goodman 2015)

[147] Cerrudo (2015)

[148] For example, Goodman (2015) details a case where an ex-employee altered the database records of a car sales company who were using GPS trackers and remote control boxes to re-possess cars, randomly disabling cars and setting off their alarms.

[149] Perlroth (2015)

[150] Markey and Waxman (2013); all five commissioners of the Federal Energy Regulatory Commission (FERC) agree that the threat of a cyber-attack on the electric grid is the top threat to electricity reliability in the United States.

[151] Paganini (2013)

[152] Prince (2014)

[153] Prince (2014)

[154] Perlroth (2015)

[155] Reilly (2015)

[156] Reilly (2015)

[157] Verizon's 2013 Data Break Investigators Report, cited in Goodman (2015)

[158] Trustwave cited in Goodman (2015)

[159] www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[160] Goodman (2015)

[161] Singer and Friedman (2014)

[162] Rainie *et al*. (2014)

[163] Townsend (2013); Kitchin (2014a)

[164] Singh and Pelton (2013)

[165] The Center for the Study of the Presidency and Congress (2014)

[166] Singh and Pelton (2013)

[167] The Center for the Study of the Presidency and Congress (2014)

[168] Townsend (2013)

[169] Brewster (2014)

[170] Cox (2014)

[171] Cerrudo (2015)

[172] Goodman (2015: 228)

[173] For example, RFID chips can be hacked, jammed and spoofed (Goodman 2015)

[174] Singh and Pelton (2013)

[175] The Center for the Study of the Presidency and Congress (2014)

[176] Goodman (2015)

[177] The Center for the Study of the Presidency and Congress (2014)

[178] Nanni (2013); Krebs (2015)

[179] Vijayan (2014)

[180] Vijayan (2014)

[181] Vijayan (2014)

[182] In the case of the Target data breach in which over 100 million customer details were stolen it appears that the retailer did not properly segment its data network, with hackers gaining access

through the company that maintained its heating, ventilation and air conditioning (HVAC) system (Vijayan 2014)

[183] Paganini (2013)

[184] Leitner and Capitanini (2014)

[185] Cerrudo (2014)

[186] Nanni (2013); Goodman (2015)

[187] Somewhat worryingly a security audit of FAA air traffic control networks uncovered 763 high risk vulnerabilities (Goodman 2015)

[188] A recent Wired article details how two hackers were able to remotely hack a car through its Internet computer that controls entertainment and navigation systems, facilitates phone calls and can provide a wifi hotspot, using it as a route to replace firmware that enabled them to take control of the car's internal computer network. The hackers could then take over the driving of the car from over 10 miles away, turning the driver into a passenger. (Greenburg 2015)

[189] Data visualisation: www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/; Spreadsheet of data and sources: https://docs.google.com/spreadsheets/d/1Je-YUdnhjQJO_13r8iTeRxpU2pBKuV6RVRHoYCgiMfg

[190] Ponemon Institute (2014)

[191] Ponemon Institute (2014); Goodman (2015)

[192] Goodman (2015)

[193] Finklea (2014)

[194] Brenner (2014); Prince (2014)

[195] Ponemon Institute (2014)

[196] Ponemon Institute (2014)

[197] Prince (2014)

[198] Prince (2014)

[199] Prince (2014)

[200] Cerrudo (2015); Lomas (2015)

[201] Cerrudo (2015)

[202] Chief Information Officer, Chief Technology Officer

[203] Cerrudo (2015)

[204] Cerrudo (2015)

[205] Peters (2015)

[206] Perrow (2014) argues that multiple and unexpected failures are inherently built into the complex and tightly-coupled technological systems. Beyond any malicious intent, such systems are prone to what he terms 'normal accidents' (e.g., bugs, human errors) that can make them malfunction.

[207] Santucci (2013)

[208] Cohen, J. (2012: 2)

[209] Cavoukian (2009)

[210] Tarin (2015)

[211] Schneier (2015)

[212] Rambam (2008); Rubenking (2013)

[213] Cohen, J. (2012); Solove (2007)

[214] Schneier (2015)

[215] As Angwin's (2014) concerted attempts to reclaim her privacy highlight, at present it is very difficult to regain any meaningful level of protection or redress with respect to the mass generation of big data. Despite being technically savvy and having access to leading experts in the field she struggled to find technical solutions that limited the data generated about her.

[216] Angwin (2014: 223)

[217] Cavoukian *et al*. (2010: 276)

[218] Minelli *et al.* (2013); Mayer-Schonberger and Cukier (2013)

[219] Article 29 Data Protection Working (2014); Fuster and Scherrer (2015)

[220] Brenner (2014); Prince (2014)

[221] Angwin (2014)

[222] Martínez-Ballesté *et al*. (2013); Cerrudo (2015); also see https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[223] 'Promoting Data Protection by Privacy Enhancing Technologies (PETs)', COM(2007) 228 final cited in European Data Protection Supervisor (2014)

[224] https://en.wikipedia.org/wiki/Privacy-enhancing_technologies

[225] See https://cyberlaw.stanford.edu/wiki/index.php/PET for a list of PETs

[226] Martínez-Ballesté *et al*. (2013)

[227] The White House (2012); Article 29 Data Protection Working (2014); FTC (2000); Ramirez (2013); Lomas (2015); New Zealand Data Futures Forum (2014); CIPPIC (2006)

[228] Crawford and Schultz (2014)

[229] Article 29 Data Protection Working Party (2014); Lomas (2015)

[230] Crawford and Schultz (2014)

[231] Cavoukian (2009)

[232] Cavoukian *et al*. (2010)

[233] Cavoukian (2009); Murphy (2015)

[234] Lomas (2015)

[235] Cerrudo (2015)

[236] Article 29 Data Protection Working Party (2014)

[237] Kansas City formed a smart city advisory in August 2015, but there are few details available publicly. kcmayor.org/newsreleases/mayor-james-names-smart-city-advisory-board

[238] smarterlondon.co.uk/about/smart-london-board/

[239] www.london.gov.uk/sites/default/files/smart_london_plan.pdf

[240] Carson (2014); Goldsmith (2015)

[241] www.seattle.gov/information-technology/privacy-program

[242] Seattle.gov (2014)

[243] Goldsmith (2015)

[244] www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf

[245]www.seattle.gov/Documents/Departments/InformationTechnology/privacy/CityOfSeattlePrivacyStatementFINAL.pdf

[246] Seattle Privacy Coalition (n.d.) https://www.seattleprivacy.org/mission

[247] Nanni (2013)

[248] Cerrudo (2015)

[249] Chief Information Officer, Chief Technology Officer, and Chief Data Officer.

[250] https://tfl.gov.uk/corporate/about-tfl/how-we-work

[251] https://tfl.gov.uk/corporate/privacy-and-cookies/privacy-and-data-protection-policy

[252] TFL - content.tfl.gov.uk/eops-schedule2-appendix24-data-retention.pdf

[253] Nanni (2013)

[254] Ken Munro - https://www.pentestpartners.com/blog/ethical-disclosure-and-the-internet-of-things/

[255] Cerrudo (2015)

[256] Ponemon Institute (2014)

[257] Hosted in the Department of Communications, Energy and Natural Resources. www.dcenr.gov.ie/communications/en-ie/Internet-Policy/Pages/National-Cyber-Security-Centre.aspx

[258] https://www.iriss.ie/iriss/

References

Andrejevic, M. (2013) *Infoglut: How Too Much Information is Changing the Way We Think and Know*. Routledge, New York.

Angwin, J. (2014) *Dragnet Nation*. St Martin's Press, New York.

Article 29 Data Protection Working Party (2014) *Opinion 8/2014 on the Recent Developments on the Internet of Things*. ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (last accessed 4 November 2015)

Baracos, S. and Nissenbaum, H. (2014) Big data's end run around anonymity and consent. In Lane, J., Stodden, V., Bender, S. and Nissenbaum, H. (eds) *Privacy, Big Data and the Public Good*. Cambridge University Press, Cambridge, pp. 44-75.

Batty, M., Axhausen, K.W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G. and Portugali, Y. (2012) Smart cities of the future. *European Physical Journal Special Topics* 214: 481–518.

Block, T. and Van Assche, J. (2010) Disentangling urban sustainability: The Flemish City Monitor acknowledges complexity. Paper presented at the *Seventh International Conference on Ecological Informatics: Unravelling Complexity and Supporting Sustainability*, Ghent, Belgium, December 2010. biblio.ugent.be/input/download?func=downloadFile&recordOId=1090655&fileOId=1090661 (last accessed 17 July 2014)

Brenner, J. (2014) Nations everywhere are exploiting the lack of cybersecurity. *Washington Post*, 24 October. www.washingtonpost.com/opinions/joel-brenner-nations-everywhere-are-exploiting-the-lack-of-cybersecurity/2014/10/24/1e6e4b70-5b85-11e4-b812-38518ae74c67_story.html (last accessed 19 Oct 2015)

Brewster, T. (2014) Smart or stupid: will our cities of the future be easier to hack? *The Guardian*, 21 May. www.theguardian.com/cities/2014/may/21/smart-cities-future-stupid-hack-terrorism-watchdogs (last accessed 21 November 2015)

Caragliu, A., Del Bo, C., and Nijkamp, P. (2009) *Smart Cities in Europe*. Series Research Memoranda 0048. Amsterdam: VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics.

Carson, A. (2014) Seattle Launches Sweeping, Ethics-Based Privacy Overhaul. *The Privacy Advisor*, 7 November (last accessed 12 October 2015)

Cavoukian, A. (2009) *Privacy by Design: A Primer*. www.privacybydesign.ca/content/uploads/2013/10/pbd-primer.pdf (last accessed 15 October 2013)

Cavoukian, A. and Castro, D. (2014) *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*. Information and Privacy Commissioner Ontario, Canada. www2.itif.org/2014-big-data-deidentification.pdf (last accessed 20 November 2015)

Cavoukian, A., Polonetsky, J. and Wolf, C. (2010) SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society* 3(2): 275-294.

Cerrudo, C. (2014) Hacking US (and UK, Australia, France, etc.) Traffic Control Systems, *IOActive Blog*, 30 April. blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html (last accessed 12 October 2015)

Cerrudo, C. (2015) *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks*. Securing Smart Cities, securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf (last accessed 12 October 2015)

CIPPIC (2006) *On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship. A Report on the Canadian Data Brokerage Industry*. The Canadian Internet Policy and Public Interest Clinic, Ottawa. www.cippic.ca/uploads/May1-06/DatabrokerReport.pdf (last accessed 17 January 2014)

Citron, D. (2007-2008) Technological Due Process. *Washington University Law Review* 85: 1248-1313

Citron,D. and Pasquale, F. (2014) The Scored Society: Due Process for Automated Predictions. *Washington Law Review* 89: 1-33

Cohen, B. (2012) What Exactly Is A Smart City? *Fast Co.Exist*, 19 September, www.fastcoexist.com/1680538/what-exactly-is-a-smart-city (last accessed 28 April 2015)

Cohen, J. (2012) What is privacy for? *Social Sciences Research Network*. papers.ssrn.com/sol3/papers.cfm?abstract_id=2175406 (last accessed 16 July 2013)

Coletta, C., Heaphy, L. and Kitchin, R. (2015) Dublin as a smart city? *Programmable City blog*, 2 December. www.maynoothuniversity.ie/progcity/2015/12/dublin-as-a-smart-city/ (last accessed 2 December 2015)

Cox, J. (2014) This Website Streams Camera Footage from Users Who Didn't Change Their Password. *Motherboard*, 31 October. motherboard.vice.com/read/this-website-streams-

camera-footage-from-users-who-didnt-change-their-password (last accessed 22 November 2015)

Crawford, K. and Schultz, J. (2014) Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review* 55(1): 93-128

Crump, C. and Harwood, M. (2014) Invasion of the Data Snatchers: Big Data and the Internet of Things Means the Surveillance of Everything. *ACLU*, 25 March. www.aclu.org/blog/speakeasy/invasion-data-snatchers-big-data-and-internet-things-means-surveillance-everything (last accessed 22 November 2015)

Datta, A. (2015) New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city, Gujarat. *Dialogues in Human Geography* 5(1): 3-22.

de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (2013) Unique in the Crowd: The privacy bounds of human mobility. *Nature*, Scientific Reports 3, article 1376: 1-5 www.nature.com/articles/srep01376.pdf (last accessed 13 November 2015)

Dodge, M. and Kitchin, R. (2005) Codes of life: Identification codes and the machine-readable world. *Environment and Planning D: Society and Space*. 23(6): 851-881.

Dodge, M. and Kitchin, R. (2007) The automatic management of drivers and driving spaces. *Geoforum* 38(2): 264-275.

Ducklin, P. (2015) The Big Data picture - just how anonymous are 'anonymous' records? *Naked Security*, 12 February. nakedsecurity.sophos.com/2015/02/12/the-big-data-picture-just-how-anonymous-are-anonymous-records/ (last accessed 16 November 2015)

Durbin, S. (2015) Building Smart City Security. *TechCrunch*, 12 September. techcrunch.com/2015/09/12/building-smart-city-security/ (last accessed 21 September 2015)

Efrati, A., Thurm, S. and Searchy, D. (2011) Mobile-App Makers Face U.S. Privacy Investigation, *Wall Street Journal*, 5 April. online.wsj.com/article/SB10001424052748703806304576242923804770968.html (last accessed 17 July 2013)

Elwood, S. and Leszczynski, A. (2011) Privacy reconsidered: New representations, data practices, and the geoweb. *Geoforum* 42: 6–15.

European Data Protection Supervisor (2014) *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*.

secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf (last accessed 4 November 2015)

Finklea, K. (2014) Identity theft: Trends and issues. *Congressional Research Service*, 21 January. www.fas.org/sgp/crs/misc/R40599.pdf (last accessed 20 November 2015)

FTC (2000) *Privacy online: Fair information practice principles in the electronic marketplace*. Federal Trade Commission, Washington DC. www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf (last accessed 16 November 2015)

Fuster, G.G. and Scherrer, A. (2015) *Big Data and smart devices and their impact on privacy*. Committee on Civil Liberties, Justice and Home Affairs (LIBE), Directorate-General for Internal Policies, European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf (last accessed 4 November 2015)

Gallagher, S. (2014) Where've you been? Your smartphone's Wi-Fi is telling everyone. *Ars Technica*, 5 November. arstechnica.com/information-technology/2014/11/where-have-you-been-your-smartphones-wi-fi-is-telling-everyone/ (last accessed 7 December 2015)

Gardham, M. (2015) Controversial face recognition software is being used by Police Scotland, the force confirms. *Herald Scotland*, 26 May www.heraldscotland.com/news/13215304.Controversial_face_recognition_software_is_being_used_by_Police_Scotland__the_force_confirms/ (last accessed 13 November 2015)

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N. and Meijers, E. (2007) *Smart cities: Ranking of European medium-sized cities*. Centre of Regional Science, Vienna UT. www.smart-cities.eu/download/smart_cities_final_report.pdf (last accessed 12 October 2015)

Goldsmith, S. (2015) Protecting big data: Seattle's digital privacy initiative aims to keep innovation on track with new data safeguards. *Data-Smart City Solutions*. 29 September. datasmart.ash.harvard.edu/news/article/protecting-big-data-742 (last accessed 22 November 2015)

Goodman, M. (2015) *Future Crimes: A Journey to the Dark Side of Technology – and How to Survive It*. Bantam Press, New York.

Graham, S. (2005) Software-sorted geographies. *Progress in Human Geography* 29(5): 562-80.

Graham, S. (2011) *Cities Under Siege: The New Military Urbanism*. Verso, London.

Graves (2015) An Exploratory Study of Mobile Application Privacy Policies. *Technology Science*, 30 October. jots.pub/a/2015103002/ (last accessed 9 November 2015)

Greenburg, A. (2015) Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired* 21 July. www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (last accessed 16 October 2015)

Greenfield, A. (2013) *Against the Smart City*. New York: Do Publications.

Hamm, D. (2013) Seattle police have a wireless network that can track your every move. *Kirotv.com*, 23 November. www.kirotv.com/news/news/seattle-police-have-wireless-network-can-track-you/nbmHW/ (last accessed 14 October 2015)

Hein, B. (2014) Uber's data-sucking Android app is dangerously close to malware. *Cult of Mac*, 26 November 26. www.cultofmac.com/304401/ubers-android-app-literally-malware/ (last accessed 13 November 2015)

Henry, A. (2013) How Retail Stores Track You Using Your Smartphone (and How to Stop It). *Lifehacker*, 19 July. lifehacker.com/how-retail-stores-track-you-using-your-smartphone-and-827512308 (last accessed 15 November 2015)

Hill, D. (2013). On the smart city: Or, a 'manifesto' for smart citizens instead. *City of Sound*, 1 February. www.cityofsound.com/blog/2013/02/on-the-smart-city-a-callfor-smart-citizens-instead.html (last accessed 5 February 2013)

Hollands, R.G. (2008) Will the real smart city please stand up? *City*, 12(3): 303-320.

Human Rights Watch (2012) *Losing Humanity: The Case Against Killer Robots*. International Human Rights Clinic, Harvard University. www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf (last accessed 17 November 2012)

Kitchin, R. (2014a) The real-time city? Big data and smart urbanism, *GeoJournal*, 79(1): 1-14.

Kitchin, R. (2014b) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences.* Sage, London.

Kitchin, R. (2015a) Data-driven, networked urbanism. *Programmable City Working Paper 14*. http://ssrn.com/abstract=2641802

Kitchin, R. (2015b) Making sense of smart cities: addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society* 8 (1): 131-136.

Kitchin, R. (2015c) The promise and peril of smart cities. *Journal of the UK Society of Computers and Law*. www.scl.org/site.aspx?i=ed42789, June

Kitchin, R. (2015d) Spatial big data and the era of continuous geosurveillance. *DIS Magazine.* dismagazine.com/issues/73066/rob-kitchin-spatial-big-data-and-geosurveillance/

Kitchin, R. and McArdle, G. (2015) The diverse nature of big data. *Programmable City Working Paper 15*, ssrn.com/abstract=2662462 (last accessed 29 November 2015)

Kitchin, R. and Dodge, M. (2011) *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press.

Kitchin, R., Lauriault, T.P. and McArdle, G. (2015) Knowing and governing cities through urban indicators, city benchmarking & real-time dashboards. *Regional Studies, Regional Science* 2: 1-28.

Kopytoff, V. (2013) Stores Sniff Out Smartphones to Follow Shoppers, *Technology Review*, 12 November. www.technologyreview.com/news/520811/stores-sniff-out-smartphones-to-follow-shoppers/ (last accessed 15 November 2015)

Krebs (2012) FBI: Smart Meter Hacks Likely to Spread, 9 April, *Krebs on Security*. krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ (last accessed 21 September 2015)

Leitner, T. and Capitanini, L. (2014) New Hacking Threat Could Impact Traffic Systems. *NBC Chicago*. www.nbcchicago.com/investigations/series/inside-the-new-hacking-threat/New-Hacking-Threat-Could-Impact-Traffic-Systems-282235431.html (last accessed 19 October 2015)

Leszczynski, A. (forthcoming) Geoprivacy. In Kitchin, R., Lauriault, T. And Wilson, M. (eds) *Understanding Spatial Media*. Sage, London

Little, R.G. (2002) Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures, *Journal of Urban Technology* 9(1): 109-123.

Lomas, N. (2015) The FTC Warns Internet Of Things Businesses To Bake In Privacy And Security. *TechCrunch*. techcrunch.com/2015/01/08/ftc-iot-privacy-warning (last accessed 19 October 2015)

Lyon, D. (2014) Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society* 1(2): 1-13.

Markey. E.J. and Waxman, H.A. (2013) *Electric grid vulnerability: Industry Response Reveal Security Gaps*
www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf (last accessed 15 November 2015)

Martínez-Ballesté, A., Pérez-Martínez, P.A. and Solanas, A. (2013) The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *Communications Magazine, IEEE* 51(6): 136 - 141

Mattern, S. (2013) Methodolatry and the art of measure: The new wave of urban data science. *Design Observer: Places*. 5 November.
designobserver.com/places/feature/0/38174/ (last accessed 15 November 2013)

Mayer-Schonberger, V. and Cukier, K. (2013) *Big Data: A Revolution that will Change How We Live, Work and Think*. John Murray, London.

Minelli, M., Chambers, M. and Dhiraj, A. (2013) *Big Data, Big Analytics*. Wiley, Hoboken, NJ

Mislove, A., Viswanath, B., Gummadi, K.P. and Druschel, P. (2010) You Are Who You Know: Inferring User Profiles in Online Social Networks. *Proceedings of the Third ACM International Conference on Web Search and Data Mining*, New York, pp. 251–260.

Morozov, E. (2013) *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems That Don't Exist*. New York: Allen Lane.

Murphy, M.H. (2015) The introduction of smart meters in Ireland: Privacy implications and the role of privacy by design. *Dublin University Law Journal* 38(1).

Nanni, G. (2013) *Transformational 'smart cities': cyber security and resilience*. Symantec, Mountain View, CA. eu-smartcities.eu/sites/all/files/blog/files/Transformational%20Smart%20Cities%20-%20Symantec%20Executive%20Report.pdf (last accessed 12 October 2015)

Narayanan, A. and Shmatikov, V. (2010) Privacy and security: myths and fallacies of 'personally identifiable information'. *Communications of the ACM* 53(6): 24-26.

New Zealand Data Futures Forum (2014) *Harnessing the social and economic power of data*. www.nzdatafutures.org.nz/sites/default/files/NZDFF_harness-the-power.pdf (last accessed 20 November 2015)

Nielsen (2014) *Smartphones: So Many Apps, So Much Time*. 7 January.
www.nielsen.com/us/en/newswire/2014/smartphones-so-many-apps-so-much-time.html (last accessed 13 November 2015)

OECD (1980) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 October 2015)

O'Neill, R. (2014) Open data's Achilles heel: Re-identification, *ZDNet*, 3 September. www.zdnet.com/article/open-datas-achilles-heel-re-identification/ (last accessed 20 November 2015)

Owens, W.A., Dam, K.W. and Lin, H.S. (eds) (2009) *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare, National Research Council, National Academic Press, Washington DC.

Paganini, P. (2013) Israeli Road Control System hacked, caused Traffic jam on Haifa Highway. *Hacker News*. 28 October. thehackernews.com/2013/10/israeli-road-control-system-hacked.html (last accessed 29 November 2015)

Pandurangan, V. (2014) On Taxis and Rainbows: Lessons from NYC's improperly anonymised taxi logs. *Medium*, 21 June. medium.com/@vijayp/of-taxis-and-rainbows-f6bc289679a1 (last accessed 22 November 2015)

Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, Cambridge, MA.

Perlroth, N. (2015) Online Attacks on Infrastructure Are Increasing at a Worrying Pace. *Bits, New York Times*, 14 October. bits.blogs.nytimes.com/2015/10/14/online-attacks-on-infrastructure-are-increasing-at-a-worrying-pace/ (last accessed 16 October 2015)

Perrow, C. (1984) *Normal Accidents: Living With High-Risk Technologies*. Basic Books, New York.

Peters, S. (2015) Smart Cities' 4 Biggest Security Challenges, 1 July, *InformationWeek: Dark Reading*, http://www.darkreading.com/vulnerabilities---threats/smart-cities-4-biggest-security-challenges/d/d-id/1321121 (last accessed 21 September 2015)

Pew Research Center (2015) U.S. smartphone use in 2015. 1 April. www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf (last accessed 13 November 2015)

Ponemon Institute (2014) *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness*. September. www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf (last accessed 19 October 2015)

Prince, B. (2014) Almost 70 Percent of Critical Infrastructure Companies Breached in Last 12 Months: Survey. *Security Week*, 14 July. www.securityweek.com/almost-70-percent-critical-infrastructure-companies-breached-last-12-months-survey

Rainie, L. and Anderson, J. (2014) *The future of privacy*. Digital Life in 2025. Pew Research Center. www.pewinternet.org/files/2014/12/PI_FutureofPrivacy_1218141.pdf (last accessed 19 October 2015)

Rainie, L., Anders, J. and Connolly, J. (2014) *Cyber Attacks Likely to Increase*. Digital Life in 2025, Pew Research Center. www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf (last accessed 19 October 2015)

Rambam, S. (2008) Privacy is dead, get over it. Presentation at the Last Hope conference, New York. www.youtube.com/watch?v=Vsxxsrn2Tfs (last accessed 15 October 2013)

Rameriz, E. (2013) The privacy challenges of big data: A view from the lifeguard's chair. *Technology Policy Institute Aspen Forum*, 19 August. ftc.gov/speeches/ramirez/130819bigdataaspen.pdf (last accessed 11 October 2013)

Reilly, S. (2015) Records: Energy Department struck by cyber attacks, *USA Today*, 11 September. www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/

Riotta, C. (2015) How Facebook and Twitter Geotagging Is Exposing Racist Trolls in Real Life. *Tech.mic*, 2 December. mic.com/articles/129506/how-facebook-and-twitter-geotagging-is-exposing-racist-trolls-in-real-life (last accessed 7 December 2015)

Rubenking, N.J. (2013) Privacy is Dead. The NSA Killed it. Now What? *PC Mag* http://www.pcmag.com/article2/0,2817,2424193,00.asp (last accessed 15 October 2013)

Rubinstein, I.S. (2013) Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, online first. idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.short (last accessed 15 July 2013)

Sarma, S. (2015) I helped invent the Internet of Things. Here's why I'm worried about how secure it is. *Politico*. www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096 (last accessed 20 November 2015)

Santucci, G. (2013) Privacy in the Digital Economy: Requiem or Renaissance? *Privacy Surgeon*. www.privacysurgeon.org/blog/wp-content/uploads/2013/09/Privacy-in-the-Digital-Economy-final.pdf (last accessed 12 November 2015)

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M. and Oliveira, A. (2011) Smart cities and the future internet: Towards cooperation frameworks for open innovation. In Domingue, J. et al. (Eds) *Future Internet Assembly*, LNCS 6656, pp. 431–446.

Seattle.gov (2014) City of Seattle launches digital privacy initiative. 3 November. murray.seattle.gov/city-of-seattle-launches-digital-privacy-initiative/ (last accessed 12 October 2015)

Schneier, B. (2015) How we sold our souls – and more – to the internet giants, *The Guardian*, 17 May. www.theguardian.com/technology/2015/may/17/sold-our-souls-and-more-to-internet-giants-privacy-surveillance-bruce-schneier (last accessed 20 November 2015)

Shelton, T., Zook, M. and Wiig, A. (2015) The 'actually existing smart city'. *Cambridge Journal of Regions, Economy and Society* 8: 13–25.

Singer, N. (2012) Mission Control, Built for Cities: I.B.M. Takes 'Smarter Cities' Concept to Rio de Janeiro. *New York Times*, 3 March. www.nytimes.com/2012/03/04/business/ibm-takes-smarter-cities-concept-to-rio-de-janeiro.html (last accessed 9 May 2013)

Singer, P.W. and Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, Oxford.

Singh, I.B. and Pelton, J.N. (2013) Securing the Cyber City of the Future. *The Futurist.* www.wfs.org/futurist/2013-issues-futurist/november-december-2013-vol-47-no-6/securing-cyber-city-future (last accessed 19 October 2015)

Solove, D.J. (2006) A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154(3): 477-560.

Solove, D.J. (2007) "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *Social Sciences Research Network*. ssrn.com/abstract=998565 (last accessed 16 July 2013)

Solove, D. (2013) Privacy management and the consent dilemma. *Harvard Law Review* 126: 1880-1903.

Soltani, A. and Gellman, B. (2013) New documents show how the NSA infers relationships based on mobile location data. *The Washington Post*, 10 December. www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/ (last accessed 14 October 2015)

Statista (2015). Number of apps available in leading app stores as of July 2015. www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (Last accessed 13 November 2015)

Strandberg, K.L. (2014) Monitoring, datafication and consent: Legal approaches to privacy in the big data context. In Lane, J., Stodden, V., Bender, S. and Nissenbaum, H. (eds) *Privacy, Big Data and the Public Good*. Cambridge University Press, Cambridge, pp. 5-43.

Stroud, M. (2014) The minority report: Chicago's new police computer predicts crimes, but is it racist? *The Verge*, 19 February. www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist (last accessed 30 November 2015)

Tarantola, A. (2014) How to Catch a Cheater Using Satellites and Cell Phones. *Gizmodo*, 22 March. gizmodo.com/how-to-stalk-a-cheater-using-satellites-and-cell-phones-1546627447 (last accessed 7 December 2015)

Tarin, D. (2015) Privacy and Big Data in Smart Cities, *AC Actual Smart City*, 28 January. www.smartscities.com/en/latest3/tech-2/item/503-privacy-and-big-data-in-smart-cities (last accessed 20 November 2015)

Tene, O, and Polonetsky, J. (2012) Big Data for All: Privacy and User Control in the Age of Analytics. *Social Sciences Research Network*. ssrn.com/abstract=2149364 (last accessed 15 July 2013)

The Center for the Study of the Presidency and Congress (2014) *Securing the U.S. Electric Grid*. Washington DC. www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf (last accessed 15 November 2015)

The Wall Street Journal (2011) What They Know – Mobile. blogs.wsj.com/wtk-mobile/ (last accessed 14 October 2015)

The White House (2012) *Consumer data privacy in a networked world: A framework of protecting privacy and promoting innovation in the global digital economy*. www.whitehouse.gov/sites/default/files/privacy-final.pdf (last accessed 29 November 2015)

Townsend, A. (2013) *Smart Cities: Big data, Civic Hackers, and the Quest for a New Utopia*. New York: W.W. Norton & Co.

U.S. Department of Energy (2004) *Blackout 2003: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf (last accessed 20 November 2014)

Vijayan, J. (2014) With the Internet of Things, smart buildings pose big risk. *Computer World*, 13 May. www.computerworld.com/article/2489343/security0/with-the-internet-of-things--smart-buildings-pose-big-risk.html (last accessed 13 November 2015)

Vincent, J. (2014) London's bins are tracking your smartphone. *The Independent*. 10 June 2014. www.independent.co.uk/life-style/gadgets-and-tech/news/updated-londons-bins-are-tracking-your-smartphone-8754924.html (last accessed 13 November 2015)

Weaver, M. (2015) Warning of backlash over car number plate camera network. *The Guardian*, 27 November. www.theguardian.com/uk-news/2015/nov/26/warning-of-outcry-over-car-numberplate-camera-network (last accessed 7 December 2015)

Weise, E. (2014) 43% of companies had a data breach in the past year. *USA Today*, 24 September. www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/ (last accessed 19 October 2015)

Wellman, T. (2015) Facial Recognition Software Moves From Overseas Wars to Local Police. *New York Times*, 12 August. www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html (last accessed 13 November 2015)

Zang, J., Dummit, K., Graves, J., Lisker, P., and Sweeney, L. (2015) Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*. October 30, 2015. http://jots.pub/a/2015103001/ (last accessed 9 November 2015)