COSMOS

Cultivate resilient smart Objects for Sustainable city applicatiOnS

Grant Agreement Nº 609043

Recommendations for IoT policy impact
WP8

Version:	1.0
Due Date:	November 30th 2016
Delivery Date:	November 30th 2016
Nature:	Report
Dissemination Level:	PU
	HILDEBRAND
Lead partner:	HILDEBRAND; LBC
Authors:	ATOS
Internal reviewers:	

www.iot-cosmos.eu

The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement n° 609043

Version Control:

Version	Date	Author	Author's Organization	Changes
0.1	30/11/2016	Joshua Cooper	HILD	HILDEBRAND, CAMDEN contributions
1.0	30/11/2016	Andrea Rossi	ATOS	Final Version

The Cosmos project consortium groups the following organizations:

Short Name	Partner Name	Country
ATOS	ATOS SPAIN SA	SPAIN
IBM ISRAEL	IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	ISRAEL
SIEMENS SRL	SIEMENS SRL	RUMANIA
ICCS	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	GREECE
SURREY	UNIVERSITY OF SURREY	UNITED KINGDOM
EMT	EMPRESA MUNICIPAL DE TRANSPORTES DE MADRID SA	SPAIN
SAMUR PC.MADRID	AYUNTAMIENTO DE MADRID	SPAIN
HILDEBRAND	HILDEBRAND TECHNOLOGY LIMITED	UNITED KINGDOM
LBC	LONDON BOROUGH OF CAMDEN	UNITED KINGDOM
III	Institute for Information Industry	TAIWAN

Deliverable Title Policy Document

Deliverable Number N/A

Keywords: Policy, Recommendations, Safety, Security, Inclusivity, Accessibility, Affordability, Ethics, Conflicts, Sensitivity.

Executive Summary: Set of IoT Policy recommendations for Camden Council to assist the public officers in creating guidelines for deployment of IoT.
The recommendations consider ethics, privacy and security in relation to IoT applications; adoption of a holistic view to the management of resources related to IoT investments (capital cost invested in the resources which create best value overall and reduce operational cost in the long term); references to building regulations for optimal health and safety and energy efficiency; legal government guidelines for dealing with the impaired, the vulnerable, children and elderly in conjunction to IoT systems; better user interfaces (in print and in digital) to ensure clearer information exchange with residents when making IoT installations.

Table of Contents

1 Policy Recommendations 4
1.1 Introduction ..... **¡Error! Marcador no definido.**
1.2 IoT Background 4
1.3 IoT Concerns 4
1.4 Safety 5
1.5 Privacy and Information Security 6
1.6 Inclusivity 7
1.7 Accessibility 7
1.8 Cultural Sensitivity 8
1.9 Affordability 8
1.10 User Conflict 8
1.11 Ethics 9
2 Policy recommendations 10
2.1 Inability to use a public service based on user type 10
2.2 Lack of security based on user type 10
2.3 Too many user names and passwords 11
2.4 Capital cost allocation 11
2.5 Operational costs and responsibility 11
2.6 Unexpected user costs 12
2.7 Buildings should be healthy 12
2.8 Building should be accessible 12
2.9 Buildings must be safe 13
2.10 Buildings must be sustainable 13
3 Appendix: UK local government functions 14
3.1 High Level Categories 14

1 Policy-related IoT topics

To assist council officers in developing policy and guidelines for the deployment of IoT, this paper sets out a set of policy issues and recommendations. In addition, examples are used successful IoT applications are presented which will help adoption by the public and council staff.

Background discussion on IoT issues is presented such that context of the technology is available to officers that are less familiar with the impact that IoT may have on council service delivery.

Where applicable a view of Building and Environmental regulation is offered as these topics were explored in detail during the COSMOS project.

1.1 IoT Background

The Internet of Things (IoT) is a self-styled term to describe objects that are able to communicate via the Internet. Objects range from sensor inputs to actuators that control physical objects with new interactions requiring advances in machine and human interfaces.

While much has been done in the area of machine to machine interfaces in the way of protocols and interoperability, the human interface has had relatively less focus.

It is probably useful to set a context with a definition of IoT provided by Haller et al.

> *A world where physical objects are seamlessly integrated into the information network, and where they, the physical objects, can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query their state and any information associated with them, taking into account security and privacy issues.*

Businesses and governments are increasingly using IoT systems to deliver their services and the information communication technology industry (ICT) industry is driving this change. It is likely that within the next 5 years IoT will touch all areas of government services.

1.2 IoT Concerns

COSMOS has considered the current challenges in IoT design, and has found that the following key areas are important factors to consider when assessing solutions, as well as constructing requirements:

COSMOS has considered the current challenges in IoT design, and has found that the following key usability areas are important factors to consider when assessing solutions, as well as constructing requirements:

Safety

> Is it safe for humans and the environment? Are there fail-safes in place to allow for any issue that may occur that can have an impact or affect on the user? What if a heating controller malfunctions? Does the device have the potential to harm the user in any way, even if it is auxiliary? Is it accessible to young children or those with learning difficulties? What could be the risk to them?

Privacy

Does the device use private data? Does it have data pertaining to the user? How is it handled? If you are using an energy monitor that shares data, it is possible to tell when the user is not at home? How are privacy issues handled, especially in the context of current discourses surrounding privacy and technology?

Inclusivity

Are you alienating certain groups of people because of certain design choices? If a service requires the user to use a social network, for example, many people may refuse to use it. Phone app vs. Web app: some users may not want to use a certain platform because it is not useful to them. Also, as a fundamental, not everyone has internet access nor a mobile/smart phone.

Accessibility

Being able to physically use something. Does it need to be moved? Does a button need to be pressed? Is it, or something it is interacting with, in a hard-to-reach place? Does it require a level of knowledge to use? Is the UI inclusive of people with certain physical or mental conditions?

Cultural Sensitivity

Have you considered how the things you are doing may be interpreted by different cultures? Disjuncture between signifier/signified - red doesn't necessarily mean danger to everyone.

Affordability

How expensive is the product/service? Does it require a lot of money to run? Do you need something expensive to enable you to use it, i.e. an iPhone or a certain spec of computer? Does this encourage elitism?

User Conflict

Does this device have the potential to create conflict between users? If multiple users can control one device, how is this handled? It might be more of an impediment than a benefit.

Ethics

Intended or unintended insight of data or functionality to enact moral judgement. If monitoring occupancy of a building for energy efficiency can indicate a resident is receiving government benefits, will rules or automation pass a moral judgement that those people should not receive heat during the day, because they should be at work.

An IoT system is not necessarily engineered to satisfy all of the concerns raised but shows the constraints and suitability of a solution and, where designers wish to engage with a particular market or end user, shortcomings can be determined.

1.3 Safety

Health and safety are fundamental to all applications, devices and measures endorsed by the EU, and every country's own health and safety requirements. It would be unethical and potentially illegal to overlook safety issues on a national or EU perspective. RAMS (Risk Assessment Method Statements) are, therefore, critical to any measure on both the level of device application, and also as an overarching basis for implementation.

Safety requirements are usually rooted in reducing the risk of fire, electric shock and injury for both the operator and laymen that might come into contact with the system. In some cases, further health and safety testing and standards may apply, including asbestos or hazardous waste substances awareness, or for small objects like sensors that might pose swallowing danger to children.

Individual devices require certification marks such as CE and UL which, in traditional electronics and telecommunication equipment, would require BS EN 60950. Each IoT device, however, especially in the case of actuators, must also require specific device safety testing using the applicable standards.

Besides the necessity of acquiring certification marks and adhering to specific quality standards, and in addition to complying to industry health and safety legislation, designers of connected products need to ensure:

- that the hardware is safe, i.e. the user is not going to get electrocuted or mistake the device for another device;
- that the product is made out of non-hazardous materials;
- that software or manual overrides are in place to ensure that it cannot:
    i. do anything to harm the user (such as a malfunctioning smart thermostat, which could leave users in unreasonably cold/damp homes because this would put them in potentially life-threatening situations, such as suffering from cardiovascular conditions or respiratory health issues); or
    ii. pose undue danger if security is compromised.

Designers have to be aware of these issues and their potential damage, and must put in place contingency plans for failures that may occur.

Safety is also crucial in the disposal of IoT equipment, such that materials do not cause environmental hazards after use and are, as far as possible, recyclable. The WEE and ROHS directives in Europe cover such issues.

Finally, feedback loops and “bad data” are likely to occur if unchecked in even a moderately simple IoT system. If actuation is taking a signal from these inputs, then malfunctions or delays in communication of a sensor may risk safety.

1.4 Privacy and Information Security

In the digital, connected realm, personal privacy has become a massive issue. Areas of concern usually stem from the risk of the misuse of private information bringing harm to an individual. That harm might be in the form of discrimination, financial loss, criminal activity, for example.

Given that IoT aims to connect our physical world, information privacy and security takes on the new dimension of a possible physical threat that can be targeted or scaled: hacking GPS traffic congestion sensors might cause traffic to falsely re-route to purposefully pose public danger; communication failure could make information inconsistent, causing a system to make harmful decisions once communication is restored; knowing a person’s travel patterns from IoT sensing might make them an easy target for identity theft or robbery.

The EU’s new General Data Protection Regulation (GDPR), adopted in April 2016 and scheduled for application in mid-2018, intends to harmonize privacy and data protection regulation

across Europe, and extends to foreign companies and agencies that process the data of EU citizens. The principles are important to put into the context of IoT:

- **Scope** – Interpretation of who and what is covered can be difficult in an IoT system, especially an IoT system that is deployed as infrastructure and reused at application layer. For instance, identification of individuals might be entrusted to an operator but, through the joining of data sets, direct or inferred personal data may still be obtained by an application utilizing that infrastructure.
- **Privacy by design** – IoT designs can be complex, and can involve many partners layered through both physical and communication spaces (through shared use assets). This part of the regulation can easily come into conflict with design for cost, safety of the commons or security requirements. In many cases, there might not be a single design authority for the entirety of the system.
- **Consent** – Data subjects (users) must be able to understand when they are giving consent to the use of their data. This consent must also be kept up to date, and its scope must not be overly broad. IoT has many use cases that are casual, and may have user interfaces that are passive, with no ability to inform users and collect their consent. It may also be hard for designers to articulate the functionality of the IoT system when reuse is an objective.
- **Right to be forgotten** – Data Subjects must be able to request the deletion of personal data relating to them that is held by a Data Controller. In certain situations, however, a Data Controller may be obliged to keep certain data, even if the Data Subject has asked for it to be deleted, i.e. in the case of financial transactions that involve tax records.
- **Data portability** – Data Subjects must be able to transfer their personal data from one electronic processing system to and into another without being prevented from doing so by the Data Controller. Accordingly, this data must be provided by the Data Controller in a structured and commonly-used electronic format.

1.5 Inclusivity

Another key usability area to consider when creating an IoT product is the inclusivity of its design. Every design decision has the potential to include or exclude users. Inclusive design emphasizes the contribution that understanding user diversity makes to informing these decisions, and thus to including as many people as possible, i.e. considering whether a design is accommodating of all people, regardless of their age, gender, mobility, ethnicity or circumstances, and avoiding the unnecessarily alienation or exclusion potential users by including or excluding particular features or specifications. This could be on the level of the language used – is it too technical? – or the usability requirements – does it require the user to have a social media account in order to participate?

1.6 Accessibility

An important facet of inclusivity is the accessibility of a product to its end user. If accessibility is viewed as the ability both to access and benefit from a product, then accessible design must

seek to maximize the universality of a product's application – making sure that a design does not exclude a specific group of potential users because their particular needs or conditions of use have not been considered. Accessibility in this sense is strongly related to universal design, which is the process of creating products that are usable by people with the widest possible range of abilities, operating within the widest possible range of situations.

The concept of accessible design focuses on enabling, as far as possible, both:

- direct access, i.e. a user's unassisted use of a product; and
- indirect access, i.e. the product's compatibility with a user's assistive technology.

If the product itself cannot be designed so that it may be directly accessed by all users, then an alternative approach for increasing its inclusivity is to ensure that it can support built-in accessibility features that might assist a user to mitigate their special needs; for example, by creating an app that supports a braille display, so that blind or visually impaired users, who might otherwise be excluded, can interact with and benefit from it.

1.7 Cultural Sensitivity

When considering the inclusivity of a design for IoT, it is also important to take into account the cultural awareness and sensitivity of a product. Today, the internet is a global platform that reaches into the homes, businesses and lives of most people on every continent. The design process of any product that looks to connect different cultures, particularly on a globalised scale, must be aware not only of cultural variances, religious practices, social mores, local customs and etiquette, but also of how certain language, concepts, symbols, motifs, colours and the placement of text and elements might be interpreted by different users.

1.8 Affordability

In order to maximise the inclusivity of IoT design still further, the affordability of a product for its end users must also be considered. The price of a product or service, especially one that is financed continuously, will affect who and how many people will be able to use it, and for how long. Additionally, if, for example, a high-specification computer or phone is required in order to support the product, access will be duly limited to an elite group of users. Other considerations include servicing, maintenance and replacement costs and requirements. In order to maintain a broad user base, it is therefore necessary to balance, as far as possible, the price of a product and its reliance on additional (costly) requirements with its efficiency, capability, profitability, etc.

1.9 User Conflict

The design of IoT products should also consider the way(s) in which these products affect users, and enable users to interact with the people around them. Many IoT devices operate in public or shared spaces, and have the capacity to be operated by multiple users. This creates the opportunity for conflict to occur between users. It is important to consider how a product might mitigate any potential for conflict, perhaps by allowing a hierarchy between users, or by granting a single user administrative privileges.

In addition, the IoT, like the Internet of People, will cause different reactions in different citizens. Some citizens will believe more in their government, local government, health service

or charitable organization. Others may well prefer their local supermarket, energy company, Facebook, Twitter or Google provider over not-for-profit organizations.

1.10 Ethics

While IoT systems themselves do not pass moral judgement, the insight gained from analyzing data in the physical world can be used unethically in three ways:

- enabling discriminatory practices that target people or locations through the IoT system e.g. identification of homeless, jobless or childless
- treating people or places with a one size fits all morality e.g. public lighting automatically shut off after midnight because the morality of the software programmer was that no one should be out late at night
- machine decisions may not be able to apply ethics and understand that there are different moral practices to be considered

In almost all cases, ethical issues arise in the design, implementation and maintenance of system logic which is performed by people. Oversight by elected officials should be maintained such that appropriate ethical consideration is given and a process to discuss and remedy ethical issues is available.

2 Policy recommendations

This section lists policy issues, recommendation and the rationale as it relates to the IoT topics in section 1. Policies may apply to different **user types** of Council services. For our discussion we have considered the following:

1. Residents – have a formal relationship with the Council, pay tax, vote and participate in election of Councillors
2. Workers – working in the borough, they have a formal tie albeit proxied through business that is operating within the Council boundaries
3. Visitors – a variety of people which at the extremes might be temporary residents staying in hotels or crossing Council boundaries while in transit. This category will be most affected by public access facilities e.g. transport hubs, local businesses, entertainment and leisure facilities

2.1 Inability to use a public service based on user type

Issue: Residents that have a formal relationship with the Council may be advantaged as they have a user identifier and electronic profile that workers and visitors may not be able to obtain. This might mean that some public services that are required, such as reporting crime may not be afforded to workers or visitors.

Recommendation: In the design of an IoT system make sure that services can either create a necessary account or be available through anonymous use. Where possible use public signage or public user interfaces to interact with IoT applications.

Rationale: Most IT systems are concerned with security and require user names. In many cases IoT applications do not actually require knowledge of the end user – in essence, physical proximity usually means you have the right to use it.

In the case of heat metering, when a new tenant moves into a property, it may be for emergency housing and therefore a housing account has not yet been set up. As a well designed IoT application, a user must be able to turn on the heat and should be given easy instructions to put credit on to a meter without restriction.

2.2 Lack of security based on user type

Issue: Validating the identity of a user may be important to ensure the security of a service; some services may not have a mechanism to validate identity due to their anonymous nature. This might make the IoT system susceptible to denial of service attacks.

Recommendation: IoT systems should use proxy identifiers carefully (MAC addresses, EUIs, etc) and corroborate identity through multiple means. Detection of conflicting readings should cause an overall error condition that is then handled appropriately in the system design.

Rationale: If an IoT system is sensing the number of people in a public space based on MAC addresses being broadcast from mobile phone Wi-Fi radios, then that should be compared with other evidence that the area is busy. For example, known rush hour or nearby CCTV analysis might be supporting evidence together with Wi-Fi signals.

2.3 Too many user names and passwords

Issue: Services that require user names and security credentials may increase the number of username and passwords to remember

Recommendation: Try to reuse credentials and identifiers where possible and prominently display functionality to securely retrieve usernames, account numbers and reset passwords. For services that require extra levels of security, PIN numbers or physical identifiers (chip and PIN) should be associated with the username and service.

Rationale: A service architecture should be used such that a single, common user identity is used with services attached, and where necessary carry additional security information. This allows for common customer care across services, reducing the contact points and costs of administration.

In the case of a new heat metering service, a payment account as well as a username and password needed to be assigned. The payment account was traditionally communicated to the user by giving them a payment card with a 13 digit number that needed to be used with the payment provider. Cards can easily be lost or unavailable to the user when they would like to make payment. A design requirement should include the ability to use the single username to make payments.

Contact Camden and the Camden Account (https://www.camden.gov.uk/ccm/navigation/council-and-democracy/about-the-council/contact-camden/) have been used for consolidation of service points and a proliferation of identities. The resident can now use the Camden Account to access their payment account number and make payments electronically.

2.4 Capital cost allocation

Issue: IoT services require power and communication infrastructure that may be too costly for a single application.

Recommendation: Identify high value services and use the business case for capital expenditure on infrastructure. Future capacity requirements should be built in to infrastructure within reason.

Rationale: Broadband within Council buildings is not widely available and due to a requirement for heat metering, housing estates received broadband for smart meter communications. Although on its own, broadband may not be justified, having a high bandwidth, reliable communications network available for IoT applications means that each service does not duplicate the broadband costs. Likewise a single sign-on username and credential service eliminates the need to invest in multiple directory services for each application.

2.5 Operational costs and responsibility

Issue: IoT services require communication and physical maintenance that may be too costly for a single application; specialist skills may be required to maintain IoT elements

Recommendation: Facilities managers should run the operating budget for the infrastructure and manage access to IT assets like they do for water, electricity and space allocation. Facilities management should also have responsibility for the maintenance and repair of IoT systems as they are typically interacting with the physical environment. This will require new skills and

authority and is a departure from IT being designated as experts because of the highly technical nature of a solution.

Rationale: Physical access and scheduling of access to homes needs to be consolidated so that multiple repairs and interactions within the homes are under one responsibility and authority. Facilities managers schedule repairs and track faults that may indicate a root cause indicated by IoT data. It is more efficient for facilities managers to coordinate the access and skills required than an IT group that is typically more inward facing to the local authority.

Facilities managers also have responsibility for performance management of buildings and will understand how data, reporting and applications can inform other processes and practices of their mechanical, electrical and sanitary specialists.

2.6 Unexpected user costs

Issue: IoT systems may generate unexpected cost to the end user

Recommendation: When implementing new IoT applications, a trial phase is suggested in order to educate users of the costs for the service; this may be implemented through an "introductory" rate or voucher based payment system giving people free credit to learn about costs for a service.

Rationale: With budget cuts, local authorities are often charging fees for council services. While this can be effective in balancing budgets and in some cases giving citizens choice in services there is a danger that users are either locked in to services or don't have appropriate interfaces to control cost of services. An example may be waste disposal whereby the council begins sending a bill for services at a flat monthly rate regardless of amount or type of rubbish collection.

2.7 Buildings should be healthy

Issue: The environment provided by a building should promote good health of the residents; while considering accessibility and safety requirements, a healthy building should be clean, warm, dry and free from pests and noise.

Recommendation: IoT applications should consider the physical effects of not only the function that they provide, but any side effects that may increase noise, allow unwanted ingress of water or pests and damage to wildlife or the natural environment.

Rationale: IoT applications often focus on the functional benefit that it provides and may not be able to sense the situation outside of sensors that inform the application. For instance, opening the window for ventilation or temperature control may not consider the outside air quality or the fact that it is raining outside; automated doors may let in vermin and increased public lighting may harm nocturnal animals or residents in houses that are near flood lighting.

In particular, The Building Regulations 2010 Part 2, Change of Use and Part 6 and Part 9 give specific tests that should be carried out. The Buildings Act 1984 Section 23 may also be of use.

2.8 Building should be accessible

Issue: Impaired or disabled residents must be able to use IoT applications where necessary for the enjoyment of a Council provided service and therefore have access to buildings and facilities.

Recommendation: Good IoT application should afford better usability regardless of someone's physical ability. Designs should limit the reliance on user interfaces through touch screens and mobile phones; alternatively, IoT solutions should sense the needs of the user and the environment with limited intervention by the user. Where setup or configuration is required, easy feedback or remote assistance should be able to be provided.

Rationale: Although society is becoming increasingly dependent on mobile phones and technology, IoT has the advantage of directly interacting with the physical environment and should be equipped with sensing that does not assume a particular user intervention.

Although there are limited national regulations on accessibility, local policy (https://www.camden.gov.uk/ccm/navigation/council-and-democracy/about-the-council/accessibility/) should be consulted.

2.9 Buildings must be safe

Issue: The automated nature of an IoT system may pose a safety risk to a user if it miscalculates or malfunctions. For example, an automated door system might endanger a user's safety by miscalculating their location and causing them injury, or by failing to recognise them and denying them access.

Recommendation: Fail-safes should be designed to mitigate or prevent potential impacts on a user's safety. In each case, fail-safe logic should be integrated as close to the actuator as possible so that it may respond quickly without disruption. Manual controls and overrides should also be implemented, with due care taken to address and account for any further safety risks that these may trigger. Use of manual controls or overrides should be evident, and should not compromise building security.

Rationale: Fail-safes are often overlooked in the design of IoT solutions, which might focus instead on a system's availability or security. They are, however, recommended as necessary to ensuring the safety of people in and around buildings and remaining in compliance with existing UK legislative requirements, specifically sections 71, 72, and 76-83 of the Building Act 1984 (http://www.legislation.gov.uk/ukpga/1984/55) and Part 8 and Schedule 1 of The Building Regulations 2010 (http://www.legislation.gov.uk/uksi/2010/2214/introduction/made).

2.10 Buildings must be sustainable

Issue: IoT systems can be wasteful. A solution that intends to promote energy efficiency might itself outweigh any cost saving or energy conservation. Alternatively, conflict between several sets of sophisticated environmental controls can create a wasteful cycle.

Recommendation: Measurement and Verification (M&V) should always be used before implementing an IoT solution to ensure benefit. Protocols such as International Performance Measurement and Verification Protocol (IPMVP) may also be used to implement a robust M&V process.

Rationale: Some costs (environmental as well as monetary) only become apparent following the implementation of an IoT solution. The M&V process ensures that these are calculated before the fact, in compliance with the regulations set out in Parts 6 and 7 and Schedule 1 of The Building Regulations 2010.

3 Appendix: UK local government functions

As a reference point, the following list of Camden Council services has been used as a prototypical local authority.

Some services are candidates for employing IoT and special attention has been given to highlight those services.

3.1 High Level Categories

- Business
- Community and Living
- Council and Democracy
- Education
- Environment
- Leisure
- Policing and public safety
- Housing
- Social Care and Health
- Transport and streets