# TGF Impact of the Internet of Things

# Introduction

As the challenges to organisations change over time, technology continuously evolves in an attempt to better address them. In particular, IT is ever developing new capabilities and extending its applicability to an increasing number of facets of business and personal life.

Forty years ago, IT was largely a set of isolated capabilities that provided local benefits to those who could afford specialized and diverse equipment and the skills to exploit it. During the 1990s, the Internet provided a universal means of joining up these islands of activity and formed the basis for a worldwide IT platform capable of organic development by a wide range of organisations and individuals. One such development was the World Wide Web that provided the ability to link information. Another, during the 2000s, was Social Media that raised the level of interworking to provide person-to-person connectivity and facilitate collaboration between individuals and organisations. These have rapidly become a part of everyday life for the public and introduced consumer-led change to business and government organisations.

The latest wave of developments takes interworking still further by incorporating objects of all sorts into the network of IT services, information, organisations and people. This is the Internet of Things (IoT) that provides the potential for e-devices to be commonly built into infrastructure such as roads, vehicles, localities (e.g. smart cities), homes, livestock and even people (e.g. for measuring bodily functions). Many organizations, including governments, are realizing that there are financial, social and other benefits that are emerging though the use of networks of e-devices for the collection of data (e.g. the monitoring of people and their environment for health purposes) or raising alerts (e.g. when river levels rise). The hope is that these networks can provide better services to society at large - whilst realising the economies that are necessary to support growing and aging populations, and also ensuring sustainability and meeting social, individual, corporate, environmental, neighbourhood, regional and global needs.

There is not yet an agreed definition of IoT, but the OASIS document “Transformational Government Framework e-Health Profile” Version 1.0[[1]](#footnote-1) offers the following:-

*“a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes.*

*Note: Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.”*

This definition does not radically conflict with those offered by others and, importantly, includes the interaction with other systems and people who can use the information generated by a set of ‘things’.

Such systems are already being developed by a wide range of players across all sectors. For example, smartness is currently being built into washing machines, TVs, refrigerators and other domestic products. These have various potential uses (and concomitant risks) and could use any of a number of connections within the home, to achieve local and possibly internet-level transmission needs.

The widespread and diverse adoption of these technologies and the ‘bottom up’ development, that is necessary for the medium term development of the IoT, are key characteristics that need to be considered and managed now as near-term projects start to build an infrastructure that would be prohibitively expensive to replace.

Some very large projects are already starting to emerge - often as Smart City initiatives. The full impact of the possible future extent of IT-based support can begin to be understood by considering the work going on in Japan to rebuild complete areas following the earthquake and tsunami in 2011[[2]](#footnote-2) There, the opportunity presented by the necessity for large scale reconstruction is being taken to introduce building and home management systems (amongst other innovations) to provide a sustainable environment that contributes to society and people’s lives. In this situation, they are, in most senses, starting from scratch and are able to agree and control the development of all systems. However, this is atypical and generally the development of a smart city or equivalent ecosystem will involve a number of organisations from a range of sectors who all need to work together and who also own existing services and systems that need to coexist and interoperate. In this scenario, building and home management systems will be fitted to new buildings and retrofitted to others.

However, further independently-supplied systems need to be able to leverage the capabilities that are already implemented. An example is an e-Health system that will contribute its own set of facilities but could usefully leverage home, building and city management systems in order to deliver its full potential. Without that capability, it would be necessary to implement much of those systems’ facilities within the e-Health system leading to duplication and increased cost.

The IoT can be used to deliver many benefits but, as with any technology, it also has the potential to be abused. Examples of use and abuse are widespread and available in the media[[3]](#footnote-3).

Thus, the longer term should be considered by taking a holistic approach to all developments that involve IoT aspects. This paper identifies some areas where the emergent IoT and its application can impact programmes in which government organisations play a major part. It then goes on to relate these to existing TGF patterns in order to help government and partner organisations deliver programmes that contribute to the future rather than constraining it by delivering tomorrow’s legacy systems, today.

# Possible Impacts of IoT-based Services.

The impacts on services that use of the IoT is likely to introduce include:-

* Unpredictable Futures
* New partnership models
* Complexity for the customer
* Data Privacy and Security
* Systems Management
* Network-related Issues

Each of these is discussed in turn.

# Unpredictable Futures

As with earlier phases of IT development, the uses to which the latest technologies will be put and the way that they and the services that they enable will develop cannot be accurately predicted.

The IoT provides a number of disruptive technologies that will lead to the innovation, by all kinds of stakeholders, that is necessary to meet the challenges of the modern world. At the same time, the use of these technologies will generate new risks alongside those that always exist such as cataclysmic events, organisations’ evolution, mergers and acquisitions and new consumer desires.

The sheer amount of data that services will generate introduces further risk factors such as the difficultly in turning it into actionable information. The volume will exceed the capability of humans to act appropriately upon it and lead to many decisions being taken automatically. This introduces the potential for some key factors to be missed leading to outcomes that are suboptimal or completely wrong.

At the same time, greater data volumes lead to increased risks of data leakage that could prove catastrophic.

However, waiting to see how the technology will turn out is not an option. Businesses and governments of all sizes have problems that have to be addressed, at least in part, in the short term and the IoT has the potential to provide some of the answers.

# New Partnership Models

Services to a region or city as discussed above will need to be provided by a range of sectors and players within them. These will include government (all tiers), energy companies, transport authorities, health services, service companies, etc. as well as a range of suppliers to those organisations.

Many systems (e.g. weather and disaster management) are regional and cross government jurisdictions. Thus, federation between sectors and their services will become increasingly important in the medium to long term.

However, the IoT is being built bottom up with a range of standards (often specific to a sector) and network types.

The foundations for collaboration and orchestration within and across sectors need to be considered early on. Relationships may become very complex with a single organisation playing custodian, supplier and consumer roles within a service ecosystem.

Stakeholder organisations will all have their own objectives and channels to market and this provides them with a challenge. How do they manage their piece of the overall ecosystem and benefit from it whilst also contributing to the greater good of society at large?

Continuity of service over time is another issue that needs to be addressed in any service development as cessation of operations by any stakeholder for whatever reason would impact the overall service.

# Complexity for the Customer

IoT-based services can have many component parts and may be provided by consortia consisting of several stakeholder organisations. This complexity is bound to confuse all but the most digitally literate customers.

From the end-user (citizen or business) perspective, any multiplicity of players could give rise to several inter-related contracts and support mechanisms. Whilst variety, choice and competition are desirable market characteristics, straightforward customer access to a small number of (aggregated) systems and seamless support for them is a necessary prerequisite to service success.

Customers will wish to change suppliers. This needs to be as seamless as possible and not result in service interruptions as they will have come to depend upon the service and service interruptions could have potentially disastrous results.

**Data Privacy and Security**

Data privacy is vital. Citizens and businesses need to trust the service and must understand the benefits that they gain in return for allowing aspects of their information to be shared.

On the supplier side, there is an understandable desire to leverage the information made available to them for service improvement and marketing purposes. This needs to be very transparent, in order to retain trust, and be rigorously enforced to ensure good practice. Examples such as the recent NHS care.data situation in the UK and the general dislike by Facebook users of the new Facebook Messenger demonstrate the fragility of trust with citizens withholding assent and migration to a range of alternative messaging applications, respectively.

Such secondary use of information needs to be transparent and not be hidden in long complex service agreements that virtually no one has the time to read, let alone understand.

The retention (and possible transfer) of raw information following a customer switching to an alternative supplier needs to be addressed in service agreements.

Cybersecurity also needs to be considered. There have been localised malicious attacks on some home management systems but the threat increases exponentially in larger systems. The current issues with unsecured Wi-Fi connections will seem insignificant compared to (e.g.) interference with any element of an e-Health or power supply system.

**Systems Management**

Many of the devices (and the data that they generate) will not be in the direct control or ownership of the public sector and the management of sensors and other devices within the community raises new challenges. Device failure or exhaustion of battery power might be mildly inconvenient in many cases but in others could be fatal (e.g. in an e-Health system). It is also important to recognise that services and the components within them will need to evolve over time.

The increased use of ICT by exploiting IoT technologies will have an impact on emissions and power usage. This may be positive when other factors, such as a service reducing power costs and impacts elsewhere, are taken into account but the overall impact of all changes on the environment needs to be understood.

Policies on asset management, monitoring, maintenance, upgrades, replacement, modification, status reporting, etc. of devices need to be open and available to all.

**Network-related Issues**

Network coverage may well be an issue. There is no single answer to connectivity and a range of alternative architectures might be needed to provide appropriate coverage for IoT and other services (sometimes even implementing several to serve the same location).

Different types of network (cabled, wireless, mobile or mesh) may be required depending on the service requirements (and more than one is likely to be necessary to support a single service – e.g. a cabled wireless backbone within a property). Some technical standards already differ for implementations within offices, industrial sites, homes, data centre and other uses.

Interference between systems (e.g. between home management systems in neighbouring properties), needs to be eradicated. This is not just a spectrum issue but could also occur at the application service level as these systems will need some level of configuration. This may be initially set up by a service provider but individuals will need to configure new devices as they subsequently acquire them. This raises the potential for accidental or malicious invasiveness into other systems.

Interference also carries the risk of impacting the availability, performance or usability of a system.

# Using the TGF

The Transformational Government Framework (TGF) provides a set of patterns that together provide guidance on, and good practice for, the development, agreement and delivery of government programmes. They are relevant to all stakeholders in such programmes, including policy developers, those responsible for service design, commissioning and delivery, elected leaders, government executives, private sector partners, suppliers, voluntary sector organizations and community representatives.

The patterns are shown in the overall TGF model:-

****

The TGF patterns are fully described in the TGF standard documentation[[4]](#footnote-4).

This section addresses each of the impacts of the IoT introduced in section 2 and identifies the TGF patterns that have the most guidance to offer in addressing them. This cannot be exhaustive and is limited to the main considerations identified within this document. All of the TGF patterns should be considered throughout the enactment of government programmes - including parts that are wholly delivered and managed by the private sector. This is particularly true for the Guiding Principles [GP1], Critical Success Factors [CSF1] and Benefit Realization [BR1]-[BR5] patterns that apply throughout all aspects of any TGF program.

Thus the remainder of this section concentrates upon applicability of the key Business, Service and Technology/Digital Asset Management patterns.

# Unpredictable Futures

The major impacts introduced by the IoT in this area are technical. However, business innovation may also introduce disruptions. As described earlier, technology will always change. The TGF addresses future-proofing by means of an open governance approach that is technology-independent including the use of programme principles.

| **IoT Impact** | **Relevant TGF Pattern(s)** | **Notes** |
| --- | --- | --- |
| Disruptive technologies | [B7], [B8], [B10][T1], [T2] |  |
| Data volumes | [B3][T1], [T2] |  |
| Automated decision making | [B3], [B6], [B8], [B9], [B10][S3][T2] |  |
| Risk of data leakage | [B3][S3][T1], [T2] | A robust security architecture is an essential foundation. |

# New partnership models

The TGF is based on collaboration between the full range of stakeholders. As technology becomes pervasive in consumer and public ‘spaces’, this facet is one to which explicit ongoing attention must be paid.

| **IoT Impact** | **Relevant TGF Pattern(s)** | **Notes** |
| --- | --- | --- |
| Services not bounded within a specific jurisdiction | [B1], [B2], [B3], [B4], [B5], [B7], [B9][S1], [S2], [S3], [S4] |  |
| Stakeholder roles and collaboration | [B1], [B3], [B4], [B5], [B6], [B7], [B8], [B9][S1], [S3] |  |
| Individual stakeholder objectives | [B1], [B2], [B5][S1] |  |
| Continuity of service | [B2], [B3], [B4], [B7], [B8], [B10][T1], [T2] |  |

# Complexity for the customer

The TGF espouses a citizen-centric approach. This tenet is vital for systems that reach so far into the consumer/user space as those made possible through IoT-powered solutions.

| **IoT Impact** | **Relevant TGF Pattern(s)** | **Notes** |
| --- | --- | --- |
| Many component parts leading to complexity for the customer | [B3], [B4], [B5], [B9][S2], [S3][T2] |  |
| Inter-related contracts and support mechanisms | [B1], [B2], [B3], [B4], [B5], [B6], [B7], [B8], [B9][S1], [S2], [S3], [S4], [S5], [S6][T1], [T2] |  |
| Customer requirement to change suppliers | [B4], [B5], [B7][S1], [S3][T1], [T2] |  |

# Data Privacy and Security

The TGF identifies the need for identity and privacy management. These requirements can be exacerbated when multiple organisations are contributing towards a service that aggregates offerings from a number of sectors. The nature of IoT systems can increase the risk factors to a system still further.

| **IoT Impact** | **Relevant TGF Pattern(s)** | **Notes** |
| --- | --- | --- |
| Engendering customer trust | [B2], [B5][S2], [S3] | There are a number of perspectives that need to be continually addressed in this area.[[5]](#footnote-5) |
| Supplier leveraging of information | [B3], [B7][S1], [S3] |  |
| Transparency of information usage | [B3], [B5], [B7][S2], [S3] |  |
| Management of data following a customer switch of supplier(s) | [B3], [B4], [B5], [B7], [B9][S1], [S2], [S3], [S4], [S5][T1], [T2] |  |
| Resilience against malicious attack | [B3], [B6], [B8][S3][T1], [T2] | A robust security architecture is an essential foundation. |

# Systems Management

The TGF addresses how changes to the way in which technology and digital assets are managed to accelerate, de-risk and lower the cost of transformation programs. These principles need to be applied to components that are deployed in customer and public spaces.

| **IoT Impact** | **Relevant TGF Pattern(s)** | **Notes** |
| --- | --- | --- |
| Management of devices not under direct control of service providers | [B3], [B5], [B7][S2], [S3], [S5][T1], [T2] |  |
| Device life | [B7], [B10][S2][T1], [T2] |  |
| Power usage, emissions, sustainability | [B1], [B3], [B5], [B6][T2] |  |
| Asset policies | [B3][T1], [T2] |  |

# Network-related Issues

The TGF recognises the need for a top-level vision and architecture for future technology use. This needs to be applied across all suppliers within a system and needs to address physical features of the environment in which service components are deployed. The use of IoT technologies necessitates an emphasis on sensors and devices and the means by which they interact with each other and with other system.

| **IoT Impact** | **Relevant TGF Pattern(s)** | **Notes** |
| --- | --- | --- |
| Network architectures | [B10][T1], [T2] |  |
| Interference between systems | [B3], [B5], [B6], [B7][S3][T1], [T2] |  |
| Configuration in end-user environments | [B3], [B5], [B7][S1], [S2], [S4], [S5][T1], [T2] |  |

Nig Greenaway

Fujitsu Fellow

1st October 2014

1. The OASIS Committee Note “Transformational Government Framework e-Health Profile” Version 1.0 – see <http://docs.oasis-open.org/tgf/TGF-eHealth-Profile/v1.0/cn01/TGF-eHealth-Profile-v1.0-cn01.pdf> [↑](#footnote-ref-1)
2. The Fujitsu Scientific & Technical Journal 2014 - 4(Vol.50, No.2) “Smart Cities and Energy Management” - see <http://www.fujitsu.com/global/about/resources/publications/fstj/archives/vol50-2.html> [↑](#footnote-ref-2)
3. The BBC News Article “Tomorrow's cities - the lamp-posts watching every move” 25th September 2014 <http://www.bbc.co.uk/news/technology-28159732> [↑](#footnote-ref-3)
4. The OASIS Committee Specification “Transformational Government Framework” Version 2.0 - See <http://docs.oasis-open.org/tgf/TGF/v2.0/cs01/TGF-v2.0-cs01.pdf> [↑](#footnote-ref-4)
5. “Internet of Things Working Group: Report to PPAB” BCS 12th June 2013 - See <http://www.bcs.org/upload/pdf/iot-report-jun13.pdf> [↑](#footnote-ref-5)