The Information Commissioner's response to Ofcom's consultation 'Promoting investment and innovation in the Internet of Things'

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications Regulations 2003 (PECR). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Information Commissioner welcomes the opportunity to respond to Ofcom's consultation on 'Promoting investment and innovation in the Internet of Things'. This response focuses only on those issues which affect information rights.

The aspect of the Ofcom consultation most relevant to the Information Commissioner's work is described in section 1.3.2 of the consultation document, regarding network security and privacy of data transmitted using the Internet of Things (IoT). This relates to the ICO's responsibility to regulate the Data Protection Act 1998.

Do internet enabled devices produce personal data?

The application of data protection law to 'the internet of things' raises some difficult questions concerning the scope of data protection law. Data protection law is concerned with information that identifies or is reasonably likely to identify an individual (directly or indirectly). It is generally accepted that information about a 'personal' electronic device – for example a smart phone – collects and processes information about its user, for example location data. This means that the organisation collecting and using the information is a 'data controller' and is therefore fully subject to data protection law. However, the application of data protection law is less certain in the case of less 'personal' devices – for

example a domestic washing machine or a TV set that all the members of a household use 'anonymously'.

It is debateable whether the datasets from such devices necessarily constitute personal data about the device's (multiple) users. As a matter of good practice the Information Commissioner would recommend that the data emanating from shared devices is kept secure, used fairly for a legitimate purpose and so forth. However, unless a particular individual is identified - or is reasonably likely to be identified - by the organisation collecting the information from the device, the information will not constitute personal data and data protection law will not apply.

We invite Ofcom to consider this issue. If there is evidence that the 'internet of things' is causing privacy problems for device users that data protection law cannot resolve, then there may be a case for the introduction of industry codes of practice or other soft-law instruments that would address this.

A realistic appraisal of privacy risk is necessary. There is no doubt that some 'internet of things' applications can collect personal data that was not collected previously and might use this in relatively intrusive ways. However, this is not always the case; in privacy terms there is little difference in theory between a washing machine informing its manufacturer automatically that it has performed 10,000 washes and therefore needs a service and the machine's owner doing this by contacting the manufacturer him/herself using traditional means.

Privacy risks from IoT devices are likely to come from linking or matching data with other datasets. For instance, a device serial number might be linked to records of a person who has signed up for an extended warranty.

A privacy impact assessment can be used to find out where genuine privacy risks arise. The ICO has produced a code of practice for privacy impact assessments. Additionally, the Article 29 Data Protection Working Party's opinion on the Internet of Things recommends that IoT device manufacturers perform a privacy impact assessment before the launch of a new application.

Fair and lawful processing: the 1st Data Protection Principle

Regarding how organisations process personal data, the DPA contains 8 principles of good information handling. The 1st principle requires that any personal data processing is both lawful and fair. Fairness includes giving individuals relevant information about the purpose of any processing of personal data, and in this way transparency is a key

requirement of the DPA. Several issues pose specific challenges to fair and transparent data processing on IoT devices.

Limited physical interfaces

IoT devices typically have smaller or more limited physical user interfaces (such as display screens, keyboards or pointing devices) in comparison with more traditional consumer computing hardware, such as desktop PCs or laptops. In some cases, IoT devices may have no physical interface at all with which an individual can interact, instead relying solely on an interface provided over a network, or relying on a separate computer, with which the device has a wired connection. This can reduce the opportunity to inform users adequately about data processing, and where appropriate, gain consent.

Limited physical interfaces mean that greater reliance must be made on other means of communication, such as:

- Sales and marketing materials
- Instruction manuals
- Network-based interfaces (e.g. a web admin interface)
- Software run on other hardware connected to the IoT device (e.g. a home PC)
- Clear product design, possibly including symbols or codes printed on the device
- Widely-accepted standards and default settings

There is an increasing trend for manufacturers to offer products that 'just work' by making the configuration process as short as possible and relying on unnecessarily permissive default settings. The Information Commissioner believes that the adopting a common set of 'privacy-friendly defaults' is particularly important given the difficulty of communicating 'fair processing' information to device users and the fact that – in reality – even if the information is provided, individuals may not read it or may not understand it if they do. Therefore a commitment from the relevant industry sectors to adopt standards ensuring that data collection and usage is essentially fair, transparent and based on 'necessity' principles would be particularly valuable.

Organisational complexity

There is increasingly a potential mismatch between what a customer understands they are buying and how an IoT device will behave in practice. This situation can arise as a result of organisational complexity, and can be made worse by lack of consumer awareness of emerging

technology. The customer may have a single object marketed to them, but behind the scenes there are potentially large numbers of different parties collaborating to provide a service in addition to the physical object. This can make transparency much more of a challenge.

Some examples of the different roles which might be involved are:

- Device manufacturer
- Device owner
- Device user
- Operating system developer
- Device software developer
- Online service (e.g. web server)
- Hosting provider
- Analytics provider
- Advertising network

These roles can be fulfilled by different combinations of organisations and individuals. For instance, a large organisation might be able to fulfil many of the above roles simultaneously, but a smaller organisation might only fulfil one role, and collaborate with other organisations to provide the service in question.

This issue of organisational complexity overlaps with the field of mobile apps, where a similar diversity of possible roles exists. The Article 29 Data Protection Working Party's opinion on apps discusses some of these roles in section 3.3, 'Parties involved in the data processing'.

When a customer buys an IoT device, it may be far from obvious to them what will happen to any personal data unless significant efforts are made to inform them appropriately.

For instance, a smart TV might have the ability to collect information on viewing habits, in order for this information to be analysed so that recommendations on what to watch next can be provided to the viewer. The viewer might well assume that the manufacturer of the TV is responsible for all of the above, when in fact the manufacturer might have a much more passive role, perhaps passing the information on to a 3rd party for analysis. In turn, this 3rd party might make use of other organisations providing services such as hosting.

In the emerging IoT market, many organisations may be expanding from an original field of expertise, to begin collecting and processing personal data where they haven't historically done so. This means they may not be experienced in dealing with data protection concerns, and so awareness-raising is important.

Innovations in providing privacy information

Privacy information need not be provided using just one method – a combination of different methods can be used. For instance, a manufacturer of an IoT device might develop a novel user interface to convey basic privacy information, while also separately providing a more detailed privacy policy on their website.

There is no requirement in the DPA to provide information in a particular format or using a particular method, and the methods used to convey privacy information can be as innovative as the products themselves.

Default settings: privacy by design and privacy by default

'Privacy by design' is an important principle to consider when designing any system that processes personal data, and hence any IoT device. The more limited the physical interface is, and the more complicated the underlying technical situation is, the more important it is that the device embodies the principle of privacy by design. This will involve taking privacy into consideration at the earliest stages of design, considering issues including data minimisation, data accuracy and retention periods. (These issues relate to the 3rd, 4th and 5th data protection principles in the DPA).

'Privacy by design' often goes hand-in-hand with 'privacy by default'. For instance, a device can have privacy features available, and yet may not be as privacy-friendly as it could be because those features are not enabled by default. For instance, an IoT device that shares data by posting status updates on a social media account would be more privacy-friendly if this feature were not enabled by default, instead requiring activation by the user.

Default settings of IoT devices will therefore be crucially important when assessing their privacy impact.

Difference between volunteered data collection and observed data collection is important

The ICO's Big Data report highlights another issue that is relevant to IoT devices that collect and process data on a large scale: namely the trend towards using observed, derived or inferred data, rather than data which has been directly provided by an individual.

It is particularly important to consider this type of processing when informing consumers, since it will be much less obvious if and when processing occurs.

Data security: the 7th Data Protection Principle

The DPA's 7th data protection principle requires organisations to take appropriate technical and organisational measures against unlawful or unauthorised data processing and against accidental loss or destruction of personal data. IoT devices raise some specific issues about information security which are relevant to the 7th principle. Organisational complexity can make these issues more difficult to appreciate and address.

Alternative interfaces may present new entry points for attackers

If a device has no physical screen or other interface, the manufacturers may for instance provide a web interface which in turn requires a network service to be running on the device and therefore relies on the software developers writing a secure interface.

If an IoT device is configured by connecting to a separate computer (for instance using a USB connection) then the configuration software running on the computer will need to be coded securely.

Other interfaces may similarly present security risks which need to be managed. It is important that anyone designing an IoT device is fully aware of any such risks.

Risk of critical software vulnerabilities not being applied

As with any product which relies on software for its operation, an IoT device risks becoming increasingly insecure if adequate software update procedures are put in place. This would typically involve at least:

- a procedure for accepting reports of security bugs and fixing them;
- a way of making software updates available;
- a way for the device in question to check for updates and apply them.

If these issues are not adequately addressed, then users' personal data could be put at risk. For instance, if someone discovers a security flaw in

the device's software, there is a risk that it might not be clear whose responsibility it will be to fix it, or how this fix will be applied. If no action is taken, such a flaw could allow an attacker to compromise the device.

In addition, publicly-available databases already exist (such as Shodan) which enumerate vulnerabilities in internet-connected devices, and this could make an attacker's job much easier.

It is important the manufacturers of IoT devices deal effectively with security updates for any relevant software, and do not expect to simply develop code once, then never have to maintain it.

Limited interfaces pose risks to secure, encrypted communications using SSL / TLS

SSL and TLS are protocols widely and effectively used to set up secure encrypted communications in order to protect data in transit. It will generally be appropriate to use an SSL / TLS connection where it is necessary to transmit any sensitive personal data, user login credentials or unique identifiers.

Limited interfaces on IoT devices risk jeopardising the security of SSL / TLS connections, for the following reasons:

- It may not be clear whether data is being transferred using an encrypted connection at all.
- There may be limited ability to warn a user of potentially insecure connections, for instance because of an invalid certificate being presented.
- Even where user warnings are possible, an unfamiliar interface may make these warnings less effective.
- The above-mentioned software update problems may also cause difficulties with keeping the device's list of trusted Certificate Authorities (CAs) up-to-date, or dealing with certificate revocation. This means an IoT device may trust a certificate when it shouldn't.

It is therefore important that software developers for IoT devices produce code which correctly sets up SSL / TLS connections where they are necessary.

Potentially increased data collection leads to greater consequences in the event of a data breach

IoT devices enable gathering and storage of greater amounts of data than were previously possible. Whether this data is stored locally or transferred elsewhere (or both) it is a target for attackers and therefore makes the potential consequences of data breach more severe.

Software lifecycles are potentially shorter than the expected lifetime of an IoT device

Many IoT devices will be performing well-established functions and hence will be expected by consumers to have a lifespan at least as long as a non-computerised, non-networked version of the same device. For instance, the lifespan of a white goods item might easily be expected to stretch to 10 years or beyond, yet it's very common for software projects to become unsupported (meaning that security updates are no longer provided) well before 10 years has passed.

Without a software development lifecycle that matches the lifecycle of the device overall, there is the possibility of an IoT device presenting an ever-increasing security risk for a matter of years between the end of software support and the point at which the device stops functioning completely or is taken out of use for some other reason.

One possible approach to software support might be for manufacturers to make the specifications of their hardware openly available, so that free / libre / open source software (FLOSS) could be written and maintained for the lifetime of the device. However, this solution depends on at least two conditions which could be difficult to fulfil in practice: firstly, the continuing availability and willingness of developers to maintain the software, and secondly, the ability of consumers to easily apply any resulting software updates.

Adoption of IPv6

The widespread adoption of IPv6 would ease the problem of limited IPv4 addresses and how they should be allocated. However, it would make IP addresses much more likely to be personal data in any given case.

This means that future engineers and software developers would need to pay greater attention to privacy and security, because they could not rely on the current assumption that a home device would be connected to a reserved (private) IP address space, behind a router performing Network Address translation (NAT).