C.T.L.R. 2018, 24(6), 139-143

Computer and Telecommunications Law Review
2018

DCMS publishes report on IoT security, privacy and safety including draft code of practice for security in consumer IoT products and associated services

Rohan Massey

David T. Cohen [1]

Subject: Information technology
Other Related Subject: Consumer law. Government administration.

Keywords: Codes of practice; Consumer protection; Cybersecurity; Department for Culture Media and Sport; Internet of things; Software; United States;

*139 Introduction

On 7 March 2018, as a key part of the UK Government's five-year, £1.9 billion National Cyber Security Strategy, which is designed to make the UK the most secure place in the world to live and do business online, and as an important piece of work linked to its Digital Charter, the Department for Digital, Culture, Media and Sport published a report entitled *Secure by Design: Improving the cyber security of consumer Internet of Things*. The report focuses on how to ensure that consumer internet-connected products—the so-called Internet of Things (IoT)—and associated services are sufficiently secure, privacy compliant and safe. It looks in detail at the rights of consumers and responsibilities of industry, mirroring the Government's Data Protection Bill and therefore the General Data Protection Regulation, which has direct effect in the UK from 25 May 2018.

Just as these new laws will require organisations that handle personal data to evaluate the risks of processing such data and implement appropriate measures to mitigate them, such measures will need to include effective cyber-security controls of consumer IoT products and associated services. To that end, the report includes a draft *Code of Practice for Security in Consumer IoT Products and Associated Services* aimed primarily at manufacturers of consumer IoT products and those developing, operating and selling IoT services and solutions.

The Internet of Things

The report explains that the IoT brings huge opportunities for citizens as well as the UK's digital economy, including increasing the functionality of many features in the home, such as remotely changing the level of heating and lighting. However, the report also states that many internet-connected devices sold to consumers lack even basic cyber-security provisions. This, paired with the rapid proliferation of these devices, has led primarily to two risks as outlined by the report:

- consumer security, privacy and safety are being undermined by the vulnerability of individual devices; and
- the wider economy faces an increasing threat of large scale cyber-attacks launched from large volumes of insecure IoT devices.

The report cites some sobering real-life examples of IoT security flaws and their consequences, including the Mirai malware which in 2016 was found to have targeted devices such as internet-enabled cameras and other IoT products, ultimately disrupting the service of many news and media websites. Exploiting common default credentials and poor configuration of the devices, the Mirai malware grouped them together as a botnet which allowed the attacker to launch a dedicated denial of service attack (DDoS) against other internet-connected devices and services. The malware was used against the French cloud computing company OVH, and the internet services company Dyn, temporarily preventing users from accessing platforms such as Netflix, GitHub and Twitter.

"Secure by design"

The report highlights the need to move away from placing the burden on consumers to securely configure their devices and towards ensuring that strong security is built into IoT devices and the services using them. It sets out the guiding principles that the DCMS regards as critical in informing future action on the part of industry and the Government to improve the security of connected devices and services. These include:

- Reducing burden (on consumers and others in the supply chain):

  As part of building security into their components, products and services, companies should reduce the burden currently placed upon consumers, and consider how they might make it easier for others in the supply chain to also implement a secure-by-design approach.

- Transparency:

  Being transparent is an essential part of a secure-by-design approach, and means explaining clearly to customers what *140 security measures have been taken, which will reduce uncertainty and increase consumer confidence when purchasing products.

- Measurability:

  In order to avoid sacrificing essential security functions in favour of functionality requirements, clear metrics should be in place that enable the assessment of the effectiveness of security measures. The report stresses the difficulty of assessing individual security measures in isolation rather than in the context of other security measures that have been put in place.

- Facilitating dialogue:

  This means maintaining effective communication across all parties across the supply chain. As different industry sectors develop their own approaches to security, underlying assumptions, models of how security is perceived, guidelines, codes of practice and regulations should all be shared widely.

- Resilience:

  This includes conducting business continuity planning, establishing a "fall-back framework" and undertaking regular risk assessments to anticipate and mitigate future problems. Clear incidence response procedures should be put in place.

Developing a Code of Practice for industry on consumer IoT

The report sets out a draft Code of Practice for industry on consumer IoT products and services. The Code is aimed at device manufacturers, IoT service providers (companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions), app developers and retailers of internet-connected products and associated services.

Three points of guidance are prioritised:

- No default passwords: All IoT device passwords must be unique and not resettable to any universal factory default value.

  The report explains that many IoT devices are being sold with universal default usernames and passwords (such as "admin, admin") which are expected to be changed by the consumer. This has been the source of many security issues in IoT, and the report suggests that the practice needs to be eliminated. To that end, best practice on passwords and other authentication methods should be followed.

- Implement a vulnerability disclosure policy: All companies that provide internet-connected devices and services must provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

  The report elaborates on this, saying that knowing about a security vulnerability allows companies to respond. It suggests that companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle.

- Keep software updated: All software components in internet-connected devices should be securely updateable. Updates must be timely and not impact on the functioning of the device. An end-of-life policy must be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons why. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

  On this third prioritised point, the report states that software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support should be made clear to the consumer when purchasing the product. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

The other proposed recommendations in the draft Code of Practice are:

- Securely store credentials and security-sensitive data:

  Any credentials must be stored securely within services and on devices. Hardcoded credentials in device software are not acceptable. ***141**

- Communicate securely:

  Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet, appropriate to the properties of the technology and usage. All keys should be managed securely. Using open, peer-reviewed internet standards is "strongly recommended".

- Minimise exposed attack surfaces:

All devices and services should operate on the "principle of least privilege"; unused ports must be closed, hardware should not unnecessarily expose access, services should not be available if they are not used, and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

- Ensure software integrity:

Software on IoT devices must be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.

- Ensure that personal data is protected:

Device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this must be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time. Consumers should also be provided with guidance on how to securely set up their device, as well as how they may eventually securely dispose of it.

- Make systems resilient to outages:

Resilience must be built into IoT services where required by the usage or other relying systems, such that the IoT services remain operating and functional.

- Monitor system telemetry data:

If collected, all telemetry such as usage and measurement data from IoT devices and services should be monitored for security anomalies within it.

- Make it easy for consumers to delete personal data:

Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

- Make installation and maintenance of devices easy:

The installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability.

- Validate input data:

Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices must be validated.

Protecting citizens' data through the Data Protection Bill

The report explains that organisations supplying IoT products and services that collect and process personal data will be subject to the requirements of the Data Protection Bill which is currently going through Parliament. They will need to consider data protection requirements carefully and take steps to address the risks posed to individuals' privacy. The report states that IoT manufacturers, in particular, need to be mindful of:

- providing clear and transparent information to consumers about what personal data devices and services process, the organisations that process this data, and the lawful basis on which the processing takes place;
- building privacy and security into the product lifecycle from the design phase and ensuring these are continued throughout;
- ensuring that appropriate technical and organisational measures are in place to protect any personal data, including processes to ensure the confidentiality, integrity, availability and resilience of processing systems and services, and regular testing to ensure the effectiveness of such measures. Organisations can ***142** consider such requirements as part of a Data Protection Impact Assessment (DPIA) where it is appropriate to do so.

Voluntary labelling scheme

The report says that the Government has identified a number of areas where consumers could benefit from information within a product label, such as stating that the product is internet-connected, its minimum support period, and providing consistent and transparent privacy-related information (e.g. the type of personal data collected, whether it is shared with third parties and whether users can opt out of sharing). While the initial focus is on a voluntary scheme, the Government says that the issue of inconsistent and opaque language within products and services' terms and conditions "remains under consideration".

Comment

The report advocates a fundamental shift in approach by moving the burden away from consumers having to secure their internet-connected devices as an afterthought and towards embedding security in the design process itself: secure by design and privacy by default, following the NCSC Secure by Default paradigm and ensuring GDPR compliance. The report highlights the practical steps that device and component manufacturers, service providers and developers of technology products can take in order to reduce the risk of cyber-attacks. In summary, these include unique passwords on new devices, a vulnerability policy and public point of contact, encryption of sensitive data, automatic software updating, easy installation, maintenance and easy removal of personal data. IoT nevertheless presents particular privacy and security challenges. Networks of many devices involving multiple operators may be difficult to manage in terms of ensuring that security vulnerabilities are removed before they are exploited.

As the report acknowledges, keeping software updated may be complicated, especially where there are cloud updates, device updates and other service updates. The Code of Practice therefore aims "to instigate positive security change throughout the entire software supply chain". From a privacy perspective, operators using IoT devices to process consumer data may be exposed and, under the GDPR, should consider using DPIAs to ensure that risks are identified and appropriate safeguards are in place before delivery of the service. Operators will be looking to manufacturers of IoT devices and components to supply GDPR-ready products. For manufacturers, this could and should be area were competitive advantage is sought.

As well as being secure, consumers need to *feel* secure, and transparency is a key element in any secure and privacy compliant IoT strategy. In its 7 March Press Release announcing the report, the Government refers specifically to the proposed product labelling scheme that would aim to aid consumer purchasing decisions and facilitate consumer trust in companies. In the Press Release, Dr Ian Levy, the NCSC's Technical Director, likens the idea of giving high quality information at the counter to shoppers of technology products to the information given to food shoppers in relation to fat content, saying:

"The NCSC is committed to ensuring the UK has the best security it can, and stop people being expected to make impossible safety judgements with no useful information."

The report has attracted strong support from various interested parties. Alex Neill, Which? Managing Director of Home Products and Services, says that "If strong security standards are not already in place when these [smart] products hit the shelves, then they should not be sold". Julian David, the CEO of TechUK, at the same time as extolling the opportunities created by the IoT, warns against the inherent risks, saying:

"It is important that companies throughout the supply chain now adopt and build on this Code of Practice to build the trust required to drive widespread take-up of the IoT."

Mark Hughes, the CEO of BT Security, is also a staunch supporter of the proposed measures, (unsurprisingly, given BT's a key advisory role in the development of the draft Code of Practice):

"From the development of the world's first Cleanfeed filter to block child abuse images, free parental controls for broadband products and devices, to warning or blocking our customers from known malware and phishing sites, BT has been at the forefront of keeping consumers and families safe online for many years. BT is actively involved in driving standards, interoperability and security across the IoT market and will continue to provide guidance to the Government and industry around best practice for securing internet connected devices."

The UK is not alone in increasing the regulatory pressure that companies face to secure internet-connected devices. The DCMS report comes as regulators in the US, particularly the Federal Trade Commission (FTC), are also increasingly scrutinising companies' practices in this area. In 2015, the staff of the FTC issued a detailed report recommending that businesses take a series of concrete steps to enhance and protect consumers' privacy and security in connection with IoT devices, steps that are similar to many of those outlined in the DCMS report. Among the measures set forth in the FTC staff report are (1) building security into devices at the outset; (2) training employees and ensuring that security is managed at an appropriate level within the organisation; (3) ensuring that when outside service providers are hired, those providers are capable of maintaining reasonable security, and providing reasonable oversight of the providers; (4) ***143** considering a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk; (5) taking measures to keep unauthorised users from accessing a consumer's device, data or personal information stored on the network; and (6) monitoring connected devices throughout their expected life cycle, and, where feasible, providing security patches to cover known risks.

The FTC has also brought enforcement actions against companies with regard to connected devices, asserting that the companies either committed an "unfair" trade practice prohibited by the FTC Act by failing to adequately secure the devices, or committed a "deceptive" practice prohibited by the FTC Act by misrepresenting to consumers the level of security in the devices. These actions include In re ASUSTek Inc[1] and FTC v D-Link Systems Corp,[2] which alleged that the companies in question supplied internet routers that were vulnerable to hackers.

Rohan Massey

David T. Cohen

Footnotes

[1] Rohan Massey is a Partner and David T. Cohen Counsel at Ropes & Gray LLP.

[1] In re ASUSTek Inc FTC File No.142 3156 (23 February 2016).

[2] FTC v D-Link Systems Corp No.3:17-cv-00039 (N.D. Cal. September 2017).

C.T.L.R. 2018, 24(6), 139-143

End of Document