Published on *The National Law Review* https://natlawreview.com

Covington Internet of Things Update: “Secure by Design” – UK Government’s Proposed Code of Practice

Article By:

Jane Pinho

The UK government has published a *Proposed Code of Practice for Security in Consumer IoT Products and Associated Services* promoting a “secure by design” approach to designing, manufacturing and delivering internet-connected products and services. The Proposed Code forms part of the government’s National Cyber Security Strategy (2016-2021) and complements the government’s focus on making the UK a center of excellence for technological innovation through, amongst other things, its IoT UK Programme, funding research and innovation in IoT. While the Code was developed in consultation with industry, the UK government intends to make some of the guidelines enforceable through regulation. The government is seeking public comment on the Proposed Code through April 25.

The rapid proliferation of internet-connected products and services is providing exciting opportunities for business innovation and economic growth. However, it also brings concerns for governments and consumers about the potential cybersecurity risks. The UK government therefore is taking a close look at IoT devices and their associated security risks, including microphones or cameras recording individuals within their homes, compromised connected home-heating or appliances threatening physical safety, and hacked access control systems allowing burglars easy access to your home. It is against this backdrop that the government is encouraging industry to assist in combatting cybersecurity threats through the design and support of products and services.

The Proposed Code contains thirteen guidelines aimed at device manufacturers, IoT service providers, mobile application developers and retailers. In particular, these stakeholders are being asked to prioritize three guidelines:

- Unique passwords. All IoT device passwords must be unique and not be possible to reset to any universal factory default value. Consumers’ reliance on default passwords makes them vulnerable to cyberattacks and, as highlighted by the government, has been at the root of a number of recent high-profile cybersecurity incidents (e.g., the use of default passwords was exploited by the Mirai malware, which ultimately disrupted the service of many news and media websites).
- Vulnerability disclosure policy. All companies that provide IoT devices and services must provide a public point of contact as part of a vulnerability disclosure policy to facilitate reporting issues. The policy should ensure continual monitoring, identification and rectification

of security vulnerabilities in IoT products and services. There is also a procedure for reporting security vulnerabilities to the National Cyber Security Centre.
- Securely updateable software. All software components in IoT devices should be securely updateable for a period appropriate to the device. Such a period should be made known to the consumer at the point of purchase.

The remaining ten guidelines urge stakeholders to: secure storage of credentials and security-sensitive data; secure communications through appropriate encryption; minimize exposed attack surfaces; ensure software integrity; ensure the protection of personal data; make systems resilient to outages; monitor system telemetry data; make it easy for consumers to delete personal data; make installation and maintenance of devices easy; and validate input data.

The UK government also spells out a number of proposed parallel actions to support the Proposed Code. Of note is a proposed voluntary labelling scheme to aid consumer purchasing decisions and facilitate consumer trust. The government suggests that an IoT product label should include a statement that the product is internet connected and provide information on the product's minimum support period, as well as consistent and transparent privacy-related information.

The report accompanying the Proposed Code specifically references the European Commission's regulatory proposal for a pan-European cyber security certification framework only to really say that, whilst the UK remains part of the EU, the UK government will continue to engage in negotiations relating to the regulatory proposals, alongside other Member States. We summarized the European Commission's proposal last fall.

Finally, the government sounds a word of warning: it is expecting industry to take the lead in developing and implementing the Proposed Code. Should rapid progress not be realized, legislation will otherwise be on the cards.

The Proposed Code is open for comments until April 25, 2018. Details on how to respond are at paragraph 7.4.

National Law Review, Volume VIII, Number 73