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

Internet of Things: How the U.K.'s Regulatory Plans Could Raise Compliance Standards

Article By:

Huw Beverley-Smith

Charlotte H.N. Perowne

Jason G. Weiss

The U.K. government recently launched a consultation process for regulating consumer Internet of Things (IOT) security. This could have significant implications for U.S. manufacturers, given that the U.K. will remain a key sales market following Brexit.

The proposals seek to better protect consumers' privacy and online security, which can be put at risk by non-secure devices. They also recognize the urgent need to shift the onus from consumers securing their own devices and ensure that strong cybersecurity is built into these "smart" products by design. The U.K. will be one of the first countries to legislate specifically in relation to IOT security. Other countries may look to the detail of U.K. regulations and their effect, particularly if the U.K. approach becomes the *de facto* international standard.

Summary of Proposals

The U.K. government is concerned that despite the introduction of a self-regulatory Code of Practice in October 2018 (COP), there are still significant security flaws in many products on the market. The U.K. proposals seek to expand on the COP, which covers 13 areas (or outcome-focused guidelines) that are widely considered good practice, including requirements that all IOT device passwords are unique, all software is securely updatable, and users have clear transparency and control over the use of their data. The code is expected to be revised by the U.K. government at least every two years.

Scope

The U.K. government intends to define the category of consumer IOT products broadly as any "network-connectable product" sold to individual consumers for personal use. The proposed scope of the legislation is wider than commonly-termed IOT products (e.g., smart home security or heating systems) and covers most "traditional" connected consumer products as well, including mobile phones and laptops. Cars and electric chargepoints, smart meters in regulated industries, and

medical devices would all be exempt, given they are already regulated by existing legislation.

Security Requirements

It is proposed that the following security requirements, derived from the European Telecommunications Standards Institute, will be mandatory as a minimum:

1. **Banning universal default passwords in IOT products**. All IOT device passwords must be unique, not resettable to any universal factory default value and not easily guessable.
2. **Implementing a vulnerability disclosure policy**, including an accessible, transparent route for consumers to report any vulnerabilities or other issues with the security of IOT products.
3. **Providing a "defined support period**", i.e. giving transparency on the minimum length of time for which the IOT product will receive security updates.

Who Does It Affect?

The proposals cover:

1. "Producers": manufacturers, their U.K. representatives where the manufacturers are not U.K.-based, or the importers or U.K. suppliers where there are no U.K. representatives.
2. "Distributors": U.K. suppliers responsible for U.K. distribution.

The obligations include ensuring that all IOT devices meet the security requirements, maintaining thorough records of compliance and cooperating fully with the regulator.

The intended effect is that all IOT devices sold in the U.K. will have to be compliant with the security requirements, including goods imported from the U.S. and elsewhere.

Implications for Manufacturers and Their Supply Chains

The U.K.-based members of the supply chain will bear the regulatory burden. However, overseas manufacturers will be required to amend their product design and security policies in line with the regulations to meet contractual requirements with U.K. importers and distributors.

The U.K. government proposes designating a regulator that will monitor industry compliance. The proposals include the usual range of civil enforcement powers, such as fines — potentially up to 4% of annual worldwide turnover (reflecting the potential high levels of fines under the EU General Data Protection Regulation (GDPR)) — and product forfeiture, suspension, and recall. In cases of continued non-compliance, criminal sanctions could follow.

The proposals include a relatively short 9-month period to achieve compliance, which works on the assumption that producers and distributors are already preparing to meet many of these obligations.

There is a risk with all legislative developments that changes introduced will merely add to the regulatory burden for businesses without being particularly effective in addressing the underlying concerns. One factor that is not considered under the proposals, and which will continue to have a significant impact on general IOT security, is Wi-Fi security. Given that a large number of IOT devices connect to a user's home Wi-Fi, some of the security measures being proposed are somewhat redundant if the user's home network is not appropriately secured. However, in this case the

proposed legislation largely follows the code of practice already in place, and many proposals, such as eliminating default passwords, should already be common practice for producers concerned with upholding consumer safety. Pressures on businesses to meet high security standards is nothing new at this point, as demonstrated by the implementation of GDPR, the California Consumer Privacy Act and similar legislation elsewhere — and the broader rise in consumer awareness about the need to ensure security for their data.

Similarly, the EU Cyber Security Act, which came into force on 27 June 2019, set the ball rolling for developing more comprehensive, mutually recognised cybersecurity certification schemes across the EU. By contrast, the U.S. has so far failed to pass any federal legislation close to what the U.K. is proposing (for example, the IOT Cybersecurity Improvement Act of 2019 does not seem to have a clear route to passage before the U.S. presidential election later this year).

Next Steps and Further Guidance

U.S. manufacturers should monitor these developments, given the potentially significant effect on manufacturers' product design and production processes and potential impact on their supply chains with U.K. and EU distributors. The deadline for submitting responses to the Call for Views is **6 September 2020**. Responses can be provided using the online feedback survey, or by populating the feedback form and emailing directly to securebydesign@dcms.gov.uk.

National Law Review, Volume X, Number 225