CHECKLIST FOR RETAILERS OF CONNECTED PRODUCTS AND SERVICES MARKETED TO CHILDREN OR FOR CHILDREN

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

Toys and products that connect to the internet are increasingly popular with children and their parents. However, without proper protection and security, the data collected by things like smart toys, watches or connected baby monitors can be shared, viewed and used in ways that expose children to risk.

Clear standards and certification are in the process of being developed, but currently, it is difficult for retailers of connected children's products to know how to ensure that the connected products you stock are secure and don't use data inappropriately.

This security and privacy checklist has been developed to help you vet potential suppliers against a set of simple criteria to ensure that the toys they stock meet a basic standard of safety for its end user. It is not intended as a replacement for mandatory or voluntary standards that are in development but is a useful tool while these are in development.

The checklist has been informed by technical experts in both system security, penetration testing and by Consumers International's members work in digital standards, cybersecurity and product safety, principles for the internet of things and national governmental codes of practice[1].

	SECURITY	
1	Does anything over the internet that is in any way connected to the smart device • comply with the OWASP Application Security Verification Standard[2], items V1-V20, at level 1 or above? • have established methods to incorporate any updates to the standard in a timely manner?	☐ ☐
2	Are users required to • add an appropriate authentication method, such as a unique strong password[3], to their accounts when first created? • if yes, does the method offered limit the risk to the end user by taking into consideration the end user's age and the method most effective in protecting their security	☐ ☐
3	Has the smart device vendor • published a responsible disclosure programme, with a designated point of contact, for security researchers to report security issues? • committed to fixing security issues that expose user data or other information within 90 days of receiving a report?	☐ ☐
4	Have all mobile applications connected to the smart device adopted procedures to • proactively detect and remediate OWASP Mobile Application Security risks? • update affected mobile applications in a timely manner?	☐ ☐
5	Is the server infrastructure, which supports smart devices and apps communicate or interact via the Internet, safeguarded against threats as outlined in Centre for Internet Security Benchmarks?	☐

CONSUMER RIGHTS

6	For products where critical vulnerabilities pose a significant threat to the functionality or security of the product and other devices on the network and cannot be resolved in 90 days through a software or firmware update are you: • immediately withdrawing products from sale? • warning existing owners and allowing them return the product? • provide exiting owners compensation or allow them exchange the product for a secure version?	☐ ☐ ☐
7	Have you explained and made clear in advance all software updates?	☐
8	Are you supporting end-of-life products by giving product software updates that relate to security issues for a minimum of three years (starting from the date the product is sold to the user)?	☐

ENCRYPTION

9	Do all wired and wireless connections to the device, such as Wi-Fi, Bluetooth, Zigbee, Z-Wave, follow application specific, key management cryptographic guidance?	☐
10	Is all data in transit or at rest subject to strong encryption such as TLS 1.2 / 1.3, SSH 2, VPN / IPSec, PKCS #1 v 2.x, Cryptographic Message Syntax (S/MIME)?	☐
11	Is all data accessed by third parties encrypted?	☐
12	Does the hardware, firmware and software found in the smart device employ a trusted execution environment, secure storage for sensitive data such as cryptographic keys and a source of pseudo-random entropy in order to seed cryptographic operations?	☐

DATA PRIVACY

13	Does the product • have a privacy policy and terms and conditions which are easily accessible, written in language that is easily understood and appropriate for the person using the device or service? • inform users about changes in terms and conditions or privacy policies in advance and be given the opportunity to withdraw from the contract? • ensure that all connectivity, settings and options not necessary for delivering the service on any product follows privacy by design standards with users asked for their opt-in consent for data collection, transmission and sharing; and when data is used for marketing purposes? • allow users easily access and delete their data and account? • automatically erase data after a set maximum period for data retention?	☐ ☐ ☐ ☐ ☐

1 Consumer Reports, Digital Standard https://www.consumerreports.org/privacy/setting-standards-for-digital-privacy/
Securing our trust, 2017, ANEC, BEUC, Consumers International, ICRT http://www.consumersinternational.org/news-resources/news/releases/consumers-international-launches-joint-iot-principles/
Secure by design: improving the cyber security of consumer internet of things, 2018 DCMS (UK) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
Cybersecurity for connected products, 2018, ANEC and BEUC Position Paper: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf

2 OWASP, Application Security Verification Standard Project

3 Strong passwords need systems that do not allow the user change the account password without the original password, have proper password storage (e.g., using hash and a strong encryption method) and provides a clear password strength indicator (i.e Uppercase and lowercase letters, digits, Symbols, use of ASCII and UNICODE characters and no common passwords from a dictionary

Consumers International is the membership organisation for consumer groups around the world.
We bring together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly. Consumers International is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.