G7 DATA PROTECTION AND PRIVACY AUTHORITIES JOINT PAPER ON CONNECTED HOME DEVICES AND CHILDREN'S PRIVACY

INTRODUCTION

We as Data Protection and Privacy Authorities (DPAs) of the G7 recognise the growing impact that connected home devices such as smart TVs, virtual voice assistants, and other internet-enabled devices, such as connected toys, have on people's daily lives, especially children.

We are aware that these products and devices have the capability to deploy online tracking technologies. Manufacturers and industry stakeholders use online tracking technologies including cookies, tracking pixels, ETags, device finger printing, or automated content recognition (ACR), to collect and store an individual's data as they use internet-enabled connected home devices. In some cases, these processes could take place without the individual being aware that such data processing is taking place.

We recognise that connected home devices may bring benefits with the potential for individuals to have more personalised experiences or to increase accessibility. At the same time, these devices are typically designed for use in places where individuals have the highest expectation of privacy: the home. The use of online tracking technologies in these connected home devices enables the monitoring of the device owners' daily activities and behaviours, as well as those of people living with the device owner or visiting the device owner's residence. Through this monitoring, connected home devices may have the ability to collect and reveal information about individuals, including children, at a large scale[1].

Evidence from consumer insight[2], regulatory complaints, and research papers[3] highlights a range of potential data protection and privacy risks associated with connected home devices, particularly when used by children, who may be less aware of the consequences of the processing of their personal data.

CHILDREN'S PRIVACY CONSIDERATIONS FOR RESPONSIBLE DATA PRACTICES

Special considerations are needed for connected home devices that are specifically targeted at children, process children's information, or are likely to be accessed by children. We encourage manufacturers, software providers, and companies in the online tracking ecosystem to ensure that such connected home devices respect, in particular, the following principles:

[1] The smart device brands harvesting your data - Which?
[2] Internet of Things Citizen Jury Report - Information Commissioner's Office
[3] The Internet of Things - An introduction to privacy issues with a focus on the retail and home environments - Office of the Privacy Commissioner of Canada

1. Privacy by Design and Default – Geolocation and online behavioural advertising settings should be switched off by default and devices should be designed to minimise data collection by default. Default settings for features such as behavioural profiling for content or friend recommendations, account creation, and data sharing should be turned off or set to the highest possible level of privacy to avoid the tracking of children's behaviours and further safeguard against accessing inappropriate content and interactions with strangers.

2. Clear and Accessible Transparency – Ensure that the privacy policy and all other communications, including terms of service, are clear and use easily understandable language which is appropriate for the level of maturity of the child. Such communication should be conspicuous, especially when the device does not have a screen. Transparency information should be provided in smaller, easy to understand elements, and at an appropriate place and time when decisions are required. Further consideration should be given to using creative formats, such as videos, to provide this information for different age groups, and to how transparency information is delivered where there is no screen interface on a device. Appropriate notice should also be provided to parents.

3. Valid Consent Mechanisms – Provide privacy tools and consent mechanisms appropriate for children and their level of maturity (or where appropriate or legally required, consent of their parent/guardian). Connected home devices should not use deceptive design patterns to encourage the child to provide more information than reasonably necessary to access the service. Consent mechanisms should also consider the evolving capacities of the child.

4. User Control and Choice – Children and/or their parents/guardians should have meaningful choices over whether and how their data is collected and used, including clear and conspicuously displayed options on the device to accept or decline data processing, and to manage their choices on an on-going basis.

5. Lawful and Fair Data Processing – Understand the high risk associated with the processing of children's data and the importance of undertaking appropriate assessments[4] to identify harms and risks specific to children and their vulnerability. Ensure that a lawful basis for processing applies to the device and service.

6. Avoid the Passive Collection of Data – Connected home devices that can "listen" or record data should give notice or disclosures in a conspicuous manner when they are collecting personal data, so that children and/or their parents/guardians are made aware so that they can meaningfully exercise their choices over the method and use of their data.

7. Data Retention - Data lawfully collected about the child should be retained for no longer than is necessary for the purposes for which such data are processed, or to comply with legal requirements.

8. Strong Security Measures – Given the heightened sensitivity of children's personal data, companies should ensure robust security protections by default are in place including automatically and regularly updating software, providing users with sufficient control and knowledge over security settings, and preventing unauthorised access, data breaches, or misuse of personal information.

9. Accountability Across the Supply Chain – Manufacturers and service providers should take responsibility for ensuring accountability throughout the data ecosystem when sharing data, especially when working

[4] Sample Data Protection Impact Assessment: Connected Toy

with third-party suppliers or other instances where manufacturers and service providers will possibly lack control e.g. over security measures used.

10. The Best Interest of the Child - Manufacturers should consider how children are likely to engage with the connected home device and consider any further privacy-preserving needs or requirements to ensure that devices are developed to comply with the relevant jurisdictions' binding policy or law.