Sky's response to the Public Bill Committee's call for evidence into the Data Protection and Digital Information 2.0 Bill

Overview

Sky welcomes the opportunity to respond to the Public Bill Committee's call for evidence into the Data Protection and Digital Information 2.0 Bill (DPDI 2.0). As a leading media and entertainment company serving 23 million homes across the UK and Europe, Sky places huge importance in ensuring our customers can use our services in a safe and secure way. In our roles as a leading retail ISP, broadcaster and content provider, we recognise that the DPDI 2.0 allows the UK to benefit from updating aspects of the UK GDPR and the Privacy and Electronic Communications Regulations 2003 (PECR) without compromising protections. Given this, we remain strongly supportive of the overarching objectives of the Bill but we do have concerns about the application of Section 3 of the Bill, as well as specific areas in Part 1 of the Bill which could go further to unlock potential for consumers, for our industry and across the economy.

Smart Data schemes

We have serious concerns about Part 3 of the Bill which will enable the introduction of Smart Data schemes across the economy. Smart Data schemes have the potential to be valuable in certain sectors, but the Bill as drafted allows them to be introduced across a variety of sectors, including communications, energy and other utilities, insurance, retail (e.g., supermarkets) and even B2B services, without consideration of any evidence of their effectiveness in supporting customers and at what Government itself acknowledges is likely to be a very high cost to industry. Without changes to the legislation that incorporate the explicit requirement for a cost benefit analysis, led by the relevant industry regulators before their implementation, these schemes could act as a significant drag on business resource, preventing the introduction of initiatives that will truly benefit customers.

Looking at the sector in which Sky operates, the communications sector already implements practices aligned with the main objectives of Smart Data Schemes and that maintain a very high bar for supporting consumers to use data to find the best deal for them. For example, in 2020 Ofcom introduced End of Contract Notifications[1], and the sector is also in the process of introducing One Touch Switching for fixed broadband which will make it easier for customers to move between providers who operate on different networks[2]. The Government's impact assessment on smart data schemes found that communications industry alone would need to spend up to £750m to implement the schemes, without providing the evidence that this would bring additional benefits to consumers that match these implementation costs[3]. Indeed, Ofcom's conclusion to its Open Communications consultation in 2021 said that there "would be important questions to consider" before a scheme is introduced and further evidence required, and that the regulator would need to seriously consider the incremental impact a scheme like this could have above and beyond the targeted consumer measures already introduced in the sector[4]. Given this high level of existing regulatory support and the cost of providing consumers with what may be only incremental additional benefits, it is imperative that the introduction of any new and potentially expensive Smart Communications schemes should be backed by a rigorous cost benefit analysis conducted by relevant industry regulators in order to ensure that consumers receive the schemes desired benefits and industry can see concrete output for the expense. We recommend that two amendments should be added in order to achieve this, including:

- To clause 62 (4) add *The Secretary of State or the Treasury shall decide to make regulations under this section only if – (i) an impact assessment has been undertaken by or at the direction of the Secretary of State or the Treasury; and (ii) based on the findings of such impact*

[1] https://www.ofcom.org.uk/news-centre/2022/end-of-contract-notifications-driving-better-deals-for-customers
[2] https://www.ofcom.org.uk/news-centre/2021/easier-than-ever-to-switch
[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1094035/Final_stage_Impact_Assessment___Smart_Data_primary_legislation.pdf
[4] https://www.ofcom.org.uk/__data/assets/pdf_file/0018/221571/statement-open-communications.pdf

assessment, the Secretary of State or the Treasury is satisfied that the likely benefits outweigh the likely costs.

- A new clause should be added stating *(a) The Secretary of State or the Treasury may direct a competent authority to exercise the power to make provision in connection with customer data under this section. (b) Where the Secretary of State or the Treasury directs a competent authority under subsection (5)(a), reference to "regulations" under this Part means 'such conditions as the competent authority may impose in exercising the power under subsection (5)(a)' and reference to "the Secretary of State or the Treasury" means such competent authority.*

Clause 85 – notification of suspected unlawful direct marketing

We understand the impact that nuisance calls have on consumers' lives and are supportive of measures to curtail the impact of them. However, Clause 85, which places a new duty for communications service providers (CSPs) to notify the Information Commissioner about suspicious activity relating to unlawful direct marketing, will be technically complex to implement and requires clear guidance for CSPs. In particular, guidance on: (i) what constitutes 'reasonable grounds' for suspicion, (ii) the extent to which providers are expected to actively monitor their networks for this activity, and (iii) the information to be reported and follow-up actions required, would be welcomed. We note that Clause 85 of the DPDI 2.0 introduces the new regulations 26A-C to the PEC Regulations and Reg 26C obliges the Information Commissioner to publish guidance on this topic, which will be key to helping industry understand and plan to meet these obligations. We believe that the Bill should be amended to recognise the need for industry to be provided with this guidance before: (i) implementing operational processes to comply with the new Reg 26A PECR and (ii) any notification obligations commence. This would be best achieved by including an additional subsection to Reg 26A, stating that these subsections will come into force after the ICO publishes its guidance and has allowed for an implementation period of, for example, at least six months after the publication of the guidance.

Clause 79 – storing information in terminal equipment

Clause 79 of the DPDI 2.0 amends the so-called 'cookie rules' in the PEC Regulation 2003 and while we recognise the intent of Government to unlock potential benefits from the UK leaving the EU, the way in which these amendments have been drafted increase the technical and administrative complexity for business, create risks to data subjects and risk not meeting the Government's aim of reducing the prevalence of pop-up cookie banners.

Our first concern is Clause 79 (2)(a) of PECR Reg 6(2C), which provides an opt-out exception to the storage / access rule for security-related software updates. As drafted, this exception requires the ability for end-users to object to, postpone, remove or disable any such software update. This presents clear security risks to end users, as it will directly hinder businesses in rolling out important security-related updates effectively and consistently across their devices. The resulting patchwork of software versions across devices will increase the risk that known security vulnerabilities will remain unaddressed for many users and will create difficulties for businesses when providing customer support. Additionally, these requirements would be technically complex to implement (especially on devices without a screen, like broadband routers) and would require consumers to respond to more cookie-style banners, which does not align with the Government's aims to reduce these. We believe that it would be suitable for the Government to maintain the existing position (as per ICO guidance[5]) that security updates are strictly necessary and require neither an opt-out nor the ability for end-users to postpone or undo them.

Additionally, despite the fact that the storage / access rule in Reg 6(1) PECR applies broadly to any storage or access rule, many of the exceptions in clause 79 of the DPDI 2.0 are only available to

[5] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9

information society services (ISS).[6] In this context, ISS does not accurately reflect how technology and online services are delivered today and gating these exceptions behind it will limit their availability, leading to unintended consequences for businesses and increased complexity for end-users without a discernible benefit. For example, we note the ICO's guidance that while 'video on demand' (VOD) services are ISS, general broadcast services are not (even where delivered over the internet).[7] Applying, this would mean that the use of audience measurement cookies in the 'on demand' section of the BBC iPlayer app may not require consent due to the exception in Reg 6(2A), but the use of the same cookies in the live TV section of the same app would require consent. We note that the ICO's guidance also clarifies that websites which just provide information about a real-world business or service are not ISS, meaning that many small businesses operating websites to provide information about opening times or their stock or service availability could not avail of these exceptions either. Instead, policymakers should replace the use of 'information society service' in these provisions to a more generic reference to 'service'.

Reg 5A PECR - security breach reporting

The DPDI 2.0 presents an opportunity to reduce the administrative burden of PECR breach reporting for Communication Service Providers (CSPs) and the ICO while still maintaining a high standard of protection under the GDPR's breach reporting rules.

Currently, Reg 5A PECR requires CSPs to: (i) report any personal data breaches occurring in connection with their service to the ICO within 24 hours of detection and (ii) notify individuals of the breach where it is *'likely to adversely affect'* their personal data or privacy. Neither of these obligations has a materiality threshold, which contrasts with: (i) Art 33 GDPR, which requires *'a risk to the rights and freedoms of individuals'* before a breach becomes reportable to the ICO and (ii) Art 34 GDPR, which requires a '*high risk to the rights and freedoms of individuals'* before it becomes notifiable to data subjects. This means that CSPs typically report far more data breaches under PECR than the GDPR, the majority of which are trivial and involve the unauthorised disclosure of limited non-sensitive data which are quickly remedied (e.g., a single email containing a first name and address being sent to an incorrect recipient). The ICO has recognised the administrative drain of these obligations both on itself and CSPs and has chosen to effectively disapply this obligation by advising CSPs that it will not take enforcement action where they fail to meet the 24-hour reporting deadline for low-risk incidents, so long as these incidents are notified within 72 hours of detection.[8] While we support the ICO's position as one which genuinely reduces the administrative burden for organisations without undermining protections for individuals, we note the uncertainty created by these obligations remaining in law while being disapplied in practice. As such, we would invite policymakers to formally remove this reporting requirement for CSPs through the introduction of a new clause to the Bill. This removal received broad support from across industry and with government prior to publication and therefore we would hope that its removal would be uncomplicated and widely supported.

Sky supports the objectives of the Data Protection and Digital Information 2.0 Bill and agrees with the Government's ambitions to cut down aimless paperwork for businesses and reduce cookie pops-ups. We believe the amendments we have suggested are proportionate and effective and will help achieve the Government's ambitions. We hope that the Committee agrees with our assessment and looks to incorporate these amendments during Committee Stage.

[6] See Regs 6(2A), (2B), (5) and (7) as set out Para 79 of DPDI 2.0.
[7] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code2
[8] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/update-on-the-ico-s-change-of-approach-to-regulating-communication-service-providers/