Written evidence submitted by ISPA. To the DATA PROTECTION AND DIGITAL INFORMATION (No. 2) Public Bill Committee, (DPDIB17).

About ISPA

1. The Internet Services Providers' Association (ISPA) is the trade association for providers of internet services in the UK. ISPA has approximately 200 members, 90% of which are SMEs, as well as large multinational companies. Our members provide internet access, hosting and a wide range of other services to consumers and businesses and we represent a wide eco-system of providers including those that build their own networks and those that resell services via fixed and wireless networks.

Summary of Main Points

In summary, to ensure a more proportionate implementation of the new requirements that strike a fair balance we are calling for:

- The provision of clearer definitions regarding the context of “unlawful”, “direct marketing”, “reasonable grounds”, and “suspicious”.
- The removal of clause 85 or a commitment to ensure that it sufficiently captures all relevant parts of the internet value chain.
- A push for a streamlined reporting process to provide industry with greater clarity to help manage the growing and competing requirements in this area.
- Clarification on whether Clause 79(2)(a)(2c) will interfere with attempts to carry out critical security updates on consumer premises equipment.
- A push for mandatory regulatory impact assessments and consultation ahead of the implementation of smart data schemes.
- Request that a formal declaration is made by Government on the independence of the Information Commission from its creation.

Introduction

2. The Data Protection and Digital Information Bill (2) is a large and highly complex piece of legislation. It brings together post-Brexit reform of the UK version of the GDPR and changes to cookie rules, with a reset of the governance framework of the Information Commissioner’s Office (ICO). The Government's intention is that the Bill will provide a “simple, clear and business-friendly framework that will not be difficult or costly to implement”.

3. The Bill has largely been presented as an attempt to reduce red tape stemming from the original GDPR and we support those parts of the Bill as long as the UK Government can ensure that the UK will retain its ability to achieve adequacy from the EU. However, our response focuses largely on the non-GDPR aspects of the DPDI Bill which in many cases actually increase red tape and go against the spirit of the overall Bill.

Unlawful Direct Marketing - A need for clear definitions

4. ISPA UK recognises that nuisance calls and unlawful direct marketing are a huge concern to consumers - tackling this issue is a major priority for our sector. The investment and time spent to address nuisance calls by providers is already recognised by Ofcom, with industry having established a Memorandum of Understanding to strengthen cooperation and reduce the impact of unlawful nuisance calls on consumers in 2020.[1] We welcome effective proposals from Government to tackle live marketing calls, and are keen to work with regulators to effect the changes necessary to bring about an end to this scourge.

5. However, we would highlight that Clause 85 of the proposed legislation - which would place a duty on network providers to report "suspicious activity" relating to "unlawful direct marketing activity" - is somewhat unclear regarding the actual types of activity that providers would be expected to report. On a basic level, this relates to the lack of clarity provided in the definitions of these terms. Our members would welcome further clarification on the terminology used to define this clause, particularly regarding the types of digital communications that this will apply to - e.g., phone calls, instant messaging, sms, email - and what the "reasonable grounds" will be for those suspecting that a breach of PECR might be occurring.

6. Whilst ISPA recognises that PECR restricts unsolicited marketing by phone, fax, email, text, or other electronic message, there are different rules for different types of communication. In its current form, the new legislation would be difficult for providers to identify whether some direct marketing activity is unsolicited. For example, providers have no way of determining whether the other elements of unlawful direct marketing in PECR - e.g. lack of consent - are met, except in clear cases such as the Telephone Preference Service.

- **Recommendation**: Provide clearer definitions regarding the context of "unlawful", "direct marketing", "reasonable grounds", and "suspicious".

Unlawful Direct Marketing - A need for a whole value chain approach

7. Clause 85 appears to also be somewhat undefined with regard to the type of services that will be included in the scope of the duty to inform, and we are concerned that this will not extend to include the whole value chain of the internet ecosystem and its constituent parts. While ISPs and telecoms providers continue to have a key role in connecting consumers, they no longer fulfil the same 'gatekeeper' role that was ascribed to them in the past. Other providers play a role in facilitating "unlawful direct marketing", including a variety of companies and services that have recently started to carry out some of the functions that are necessary for the use of the internet - browsers, app stores and in certain circumstances operating systems and apps.

8. We are concerned that the impact of encryption across the value chain has also not been wholly considered in this legislation. For example, new forms of encryption to improve privacy and integrity such as DNS over HTTPS (DoH), which is being rolled out by Mozilla (Firefox) and Google (via Chrome), as well as Private Relay by Apple, increasingly reduce the visibility of what is happening online. This in turn limits the ability of ISPs to monitor DNS and assess whether information is "suspicious" or "unlawful". At a network level, providers

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0026/31859/nuisance_calls-tech-mou.pdf

only have access to high level traffic information. This relates to the ever-developing internet consisting of a complicated, multi-layered, value chain, involving both users and a variety of online services that perform different functions.

9. The increasingly complex value chain essentially forces Government, Parliament and Regulators to make a choice between the old-fashioned approach of targeting limited sets of providers, or extending regulation across the value chain. The old-fashioned approach risks being ineffective, would not result in the Government's desired outcomes, and would put an additional, and disproportionate, regulatory and financial burden on our members.

- **Recommendation**: Remove clause 85 or ensure that it sufficiently captures all relevant parts of the internet value chain.

Unlawful Direct Marketing - Regulatory duplication

10. Ofcom itself recognises that access providers have taken steps to disrupt scams – including nuisance calls – sent over their networks, with telecoms companies having existing requirements to report data on this to the regulator. Further to this, many providers are already signatories to the Home Office's voluntary Fraud Sector Charter, which seeks to reduce the impact of scams on customers and commits that telecoms companies work with Ofcom to identify and implement techniques to block scam calls. There is a real risk that providing separate data to ICO could create an unnecessary, duplicative burden.

- **Recommendation**: We would ask the Committee to push for a streamlined reporting process to help manage the growing and competing requirements in this area.

Storing information in the terminal equipment - Critical Security Updates

11. Increasing cyber security is rightly on top of the Government's agenda. Indeed, our members recognise the importance of security and have worked to uphold these standards as threats change and evolve, and as our infrastructure and services develop. ISPs play a unique role in protecting both their own network and customers, and are often the first port of call for online users. Part of this is to ensure that consumer premise equipment, e.g. routers, is up to date with the latest security requirements.

12. We are concerned that Clause 79(2)(a)(2c) potentially undermines the ability of our members to carry out critical security updates, especially in relation to zero day exploits. The wording of the clause also appears to go against NCSC guidance, which recommends that users do not delay or resist installing security updates in order to bolster defences against cyber attacks.

13. We are still waiting for Government to respond to our queries around this and would thus welcome it if the Committee could clarify whether it will still be possible to do critical security updates on consumer premises equipment.

- **Recommendation**: Clarify whether Clause 79(2)(a)(2c) will interfere with attempts to carry out critical security updates on consumer premises equipment.

Smart Data

14. We welcome the Government's publication of the enabling legislation for the extension of Smart Data initiatives across the economy with authorised third-party providers. This has been highly anticipated since the schemes were first teased in 2018, and we appreciate that there is a lot of appetite in Parliament to replicate a policy that has seen much success in Open Banking and apply it to other sectors. However, our members have raised concerns with regard to the Government's direction of travel on this measure, as well as called out its reasoning and assessment around whether there truly is a need for the introduction of smart data schemes in already highly competitive sectors, such as telecoms.

15. An area of particular concern is that the legislation does not appear to provide procedural safeguards so that the roll-out of smart data schemes is done properly and proportionally. This relates to there being no requirement in the Bill text that the Secretary of State must undertake robust impact assessments or consultations ahead of implementing smart data initiatives and mandate industry involvement in them. For our sector, the costs of such structural change to collect and supply any 'Open Communications' data would be very significant, and could only be justified if it delivered real and significant benefits to consumers.Without proper consultation with industry, the scheme could undermine the Government's objective of bolstering choice amongst consumers by instead resulting in higher prices.

16. Further to the above points, we would raise that the recently announced membership of the UK's Smart Data Council is a concerning development. The absence of any telecoms industry representation on the Council, despite explicitly calling our sector out as a priority to "replicate the success of Open Banking in", demonstrates a further potentially concerning direction of travel by Government. Without clear industry involvement in exploring how these new ways of extending Smart Data will be delivered to new sectors, it is difficult to imagine how Government intends to explore its benefits.

    Recommendations: We would ask the Committee to push for mandatory regulatory impact assessments and a consultation ahead of implementation of smart data schemes.

Reform to the Information Commissioner's Office

17. ISPA welcomes the commitment to reform the ICO as the data protection watchdog, and shares and supports the ambition of the reforms. However, we are concerned that the current proposals risk undermining the independence of the new Commission and that Government could provide itself with too much power to steer the day-to-day decision-making of the new body.

- **Recommendation**: Request that a formal declaration is made by Government on the independence of the Information Commission from its creation.

Conclusion

18. We are broadly supportive of the new legislation, but, as set out above, we believe that it
19. can be strengthened in several areas. We hope the Committee finds the briefing paper of use.

We would be happy to follow up on any of the points raised, should there be any questions.

May 2023.