10 St Bride Street London
EC4A 4AD
T +44 (0)20 7331 2000
techUK.org | @techUK

Thursday 17 March 2022

Product Security and Telecommunications Infrastructure Public Bill Committee
Portcullis House, Bridge St
London, SW1A 2LW

Dear Chairs, Committee Members,

## techUK written submission in follow-up to evidence session

Thank you once again for asking techUK to give evidence to the Product Security and Telecommunications Infrastructure Public Bill Committee. Following the evidence session on Tuesday 15 March, I am writing to follow-up with some further information.

Firstly, Chris Elmore MP asked a question relating to Part 2 of the Bill. I explained that whilst I focus on cyber security, our Telecoms team, led by Sophie James would be delighted to share the techUK perspective. See below that response.

**Further information on fixed infrastructure (PSTI Part 2)**

The single greatest barrier techUK members in the fixed infrastructure sector face with the Electronic Communications Code (ECC) is obtaining wayleaves: our members are unable to receive access to land consents and this is the biggest constraint on rolling out full fibre broadband across the UK. This issue is caused by either unresponsive landlords, or landlords who are uncooperative. In urban areas, this issue causes difficulty in securing access to Multi Dwelling Units ("MDUs") and blocks of flats: some members point to the average time it can take to negotiate some wayleaves with landlords of tenanted properties taking two years.

There are approximately six million MDU premises in the UK: one member has shared with techUK that, in its experience of attempting to access MDUs, it estimated that potentially 25% of MDU premises would not be able to connect to fibre or gigabit broadband (1.5 million) without ECC reform.

Our members welcome the provision in the Bill for fast-tracking wayleave negotiations using an Alternative Dispute Resolution scheme. This will allow long-running negotiations for access agreement to have a meaningful backstop. These delays are often seen in negotiations with large housing associations and local authorities in urban areas, meaning a fast-tracked process will remove the potential for islands of poor digital connectivity centred on social housing stock.

It is welcome that the PSTI Bill will enable the sharing of historic wayleave agreements where infrastructure is underground. Industry sees this as a good opportunity to share the existing underground duct network (owned by BT/Openreach), which can reduce the risk of premises being cut off from a digital upgrade due to the status of their road. It is unclear if the Bill intends to address the problem of accessing poles situated above ground on private land, and industry would welcome further clarity as the Bill progresses.

However, industry feels it is a missed opportunity in that the PSTI Bill will not address the automatic upgrade and sharing rights for existing infrastructure inside blocks or flats or overground (such as poles). As currently drafted, the Bill would allow operators to use

existing duct to reach the base of such a pole, while existing provisions allow for the flying of lines between poles, but no explicit right exists to access the pole itself. In order to see the biggest benefit from this legislation, techUK members believe only small clarifications are needed to widen this scope to an already tightly defined use case.

**Further information on product security (PSTI Part 1)**

Furthermore, in addition to the briefing shared with the Committee in advance, there are a few additional points, not touched on which I thought might be useful to share with the committee regarding the product safety aspects of the bill:

**On labelling** – techUK supports DCMS' intention to utilise a digital approach to consumer communications. Increasingly consumers utilise online means to purchase and research products which allows industry to build better consumer awareness than outdated, physical labels would.

**On Security Requirement 3** - The length of software support can only ever be what the manufacture can legally commit too. It's difficult to guarantee with legal certainty how long a product can be supported because of the array of external factors, including emerging cyber threats and changing consumer habits. Companies just don't know, due to that ever-changing security landscape what the next vulnerability exploit will be.

Further engagement around this issue, including better understanding of the approach taken by the Enforcement Body to emerging threats and best endeavours is required.

**On third-party software** - If a manufacture uses recommended peer-reviewed open-source software, they might be required to keep the period of security updates shorter. More work to understand and outline the application of this legislation to Third-Party/Open-Source software is required.

**On vulnerability disclosure** - Public notification of a vulnerability should only happen once the vulnerability is fixed, to advertise vulnerabilities before a fix is applied opens the potential for consumers to be attack from lesser skilled opportunist hackers.

**On automatic patching/updates** - EN 303645 states that software updates should be automatic ideally without user interaction. Throughout purchase and lifespan of products, the focus should be on empowering consumers to better understand and engage with the resilience of their products.

techUK would be happy to answer any further queries any Committee member might have and looks forward to continuing to engage with DCMS on the relevant issues surrounding the Bill.

Yours sincerely

Dan Patefield
Head of Programme, Cyber and National Security
Dan.patefield@techuk.org

Sophie James,
Head of Programme, Telecoms and Spectrum Policy
Sophie.James@techUK.org