**Online Safety Bill "spy clause" requires Chat Platforms to Scan Private Messages** by *Dr Monica Horten*, *Open Rights Group* (16th January 2023)

The Online Safety Bill is intended to protect children from harmful content. However, it includes a requirement for private messaging (chat) services to intercept and scan the posts of every user before upload. This prospect raises deep concerns about interference with privacy and a chilling effect on freedom of expression. It's a massive expansion in surveillance capacity hidden inside the bill.

**More than 40 million British people "chat" every day:** Private messaging or chat services are a vital means of communication for many people. These services have largely replaced old-fashioned phones in daily life, whether for trade and business or messaging with extended relatives, such as grandparents. Chats are used around the clock at home, work, and leisure. There are over 40 million users in the UK on platforms such as WhatsApp, Telegram and Signal.

**Invisible measures:** The mandate for chat services to scan is almost invisible due to the obtuse drafting of the Bill. The intended meaning of 'content communicated publicly or privately' [S.203 & S.207] brings private chats into the scope of the Bill. S.110 gives Ofcom unprecedented powers to require what is, in effect, a form of mass surveillance.

**Intercept and scan private messages:** Compliance with S.110 would mean, in practice, interception and scanning of chat messages on an ongoing basis to seek out and identify images and videos in accordance with a government mandate and then remove them or prevent access. AI-based systems would look for matches of content in a database using digital fingerprints and may also use text-based classifiers. Ofcom's powers could impose 'accredited technology', a content moderation system [S.202] designed to government-approved standards [S.110].

**Compromise security of messages:** The end-to-end encryption (E2EE) that provides security for messages and guarantees confidentiality would be compromised. Likely technical solutions involve creating "back doors" in the code or scanning images on the user's phone (client-side scanning). The latter is thought to be the government's favoured approach but is not specified in the Bill. Both methods put at risk the security of messages across the whole system. It's a template that is ripe for abuse by a less benign government, a hostile state, or bad actors.

**Flawed Impact Assessment:** The government's Impact Assessment assumes stronger privacy protection that has been deleted from the Bill, reflecting a failure of due diligence in policy-making.

**Disproportionate interference with privacy:** This is a disproportionate measure, asking private companies to conduct surveillance on behalf of the State without suspicion or warrant. It's like putting a spy in everyone's pocket. It ignores less intrusive ways to address the policy aim of tackling child sexual abuse. There is no independent authorisation or oversight. The government should balance the policy aim against the intrusiveness of the measures.

**MPs are urged to drop this dystopian requirement and keep UK citizens safe from mass surveillance**.

- Delete the word "privately" and remove the "spy clause" [S.110]
- Call on the government for a full review and impact assessment of these measures

**For further information, contact the author via info@openrightsgroup.org. Contact Professor Alison Scott-Baumann for access to other experts at as150@soas.ac.uk, and visit our website for more information.** 