INDEX ON CENSORSHIP

A VOICE FOR THE PERSECUTED

SURVEILLED & EXPOSED

HOW THE ONLINE SAFETY BILL CREATES INSECURITY

NOVEMBER 2022

EXECUTIVE SUMMARY

There has been significant commentary on the flaws of the Online Safety Bill, particularly the harmful impact on freedom of expression from the concept of the 'Duty of Care'[1] over adult internet users and the problematic 'legal but harmful' category for online speech. Index on Censorship has identified another area of the Bill, far less examined, that now deserves our attention. The provisions in the Online Safety Bill that would enable state-backed surveillance of private communications contain some of the broadest and powerful surveillance powers ever proposed in any Western democracy. It is our opinion that the powers conceived in the Bill would not be lawful under our common law and existing human rights legal framework.

Index on Censorship has commissioned a legal opinion by Matthew Ryder KC, an expert on information law, crime and human rights, and barrister, Aidan Wills of Matrix Chambers. This report (a) summarises the main legal arguments and analysis; (b) provides a more detailed explanation of the powers contained in Section 104 notices; and (c) lays out the legal opinion in full.

The legal opinion shows how the powers conceived go beyond even the controversial powers contained within the Investigatory Powers Act (2016) but critically, without the safeguards that Parliament inserted into the Act in order to ensure it protected the privacy and the fundamental rights of UK citizens. The powers in the Online Safety Bill have no such safeguards as of yet.

The Bill as currently drafted gives Ofcom the powers to impose Section 104 notices on the operators of private messaging apps and other online services. These notices give Ofcom the power to impose specific technologies (e.g. algorithmic content detection) that provide for the surveillance of the private correspondence of UK citizens. The powers allow the technology to be imposed with limited legal safeguards. It means the UK would be one of the first democracies[2] to place a de facto ban on end-to-end encryption for private messaging apps. No

[1] Centre for Policy Studies (September 2020)
https://cps.org.uk/wp-content/uploads/2021/07/200926202055-SafetywithoutCensorshipCPSReport.pdf
Index on Censorship (June 2021)
https://www.indexoncensorship.org/wp-content/uploads/2021/06/Index-on-Censorship-The-Problems-With-The-Duty-of-Care.pdf

[2] https://www.hindustantimes.com/india-news/messaging-application-signal-not-in-compliance-with-new-rules-say-officials-101624508925464.html

communications in the UK - whether between MPs, between whistleblowers and journalists, or between a victim and a victims support charity - would be secure or private. In an era where Russia and China continue to work to undermine UK cybersecurity, we believe this could pose a critical threat to UK national security.

The King's Counsel's legal opinion includes that:

- **Section 104 notices amount to state-mandated surveillance** because they install the right to impose technologies that would intercept and scan private communications on a mass scale. The principle that the state can mandate the surveillance of millions of lawful users of private messaging apps should require a much higher threshold of legal justification which has not been established to date. Currently this level of state surveillance would only be possible under the Investigatory Powers Act if there is a threat to national security.
- **Ofcom will have a wider remit on mass surveillance powers of UK citizens than the UK's spy agencies**, such as GCHQ (under the Investigatory Powers Act 2016). Ofcom could impose surveillance on all private messaging users with a notice, underpinned by significant financial penalties, with less legal process or protections than GCHQ would need for a far more limited power.
- **Questionable legality:** The proposed interferences with the rights of UK citizens arising from surveillance under the Bill are unlikely to be in accordance with the law and are open to legal challenge.
- **Failure to protect journalists:** if enacted, journalists will not be properly protected from state surveillance risking source confidentiality and endangering human rights defenders and vulnerable communities.

The disproportionate interference with people's privacy identified by the legal analysis paints an altogether different picture of the Online Safety Bill. Far from being a law to establish accountability for online crime, the legislation, as drafted, opens the door for sweeping new powers of surveillance with little public debate over their purpose and proportionality. Unless the government reconsiders or parliament pushes back, these powers are set on a collision course with independent media and journalism as well as marginalised groups.

Parliamentarians should support amendments that clarify that Section 104 technology notices, or any other devices in the Bill, cannot be used to undermine end-to-end encryption. This can be achieved by accepting the amendment (153)[3] by Rt Hon David Davis MP to prevent technology notices from applying to private messaging services.

Passing the Bill in its current form risks normalising and diluting the basis for the use of online mass surveillance tools in democracies. The UK will, in essence, have conceded that authoritarian super powers like China are shaping internet standards globally[4] by allowing for the indiscriminate and disproportionate monitoring of citizens, and messages server side.

> *Today, in too many states, encryption is now essential. As we speak the reality on the ground in authoritarian regimes including China, Hong Kong, Belarus and Russia, the difference between using an encrypted messaging app to express yourself, or unencrypted communications will mean the difference between freedom and imprisonment, if not worse.*[5]

[3] https://publications.parliament.uk/pa/bills/cbill/58-03/0121/amend/onlinesafety_day_rep_0712.pdf
[4] https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/
[5] Index on Censorship (2022) Why we need to protect end-to-end encryption

KEY DEFINITIONS

Client-side scanning (CSS) or 'Surveillance Technology' broadly refers to systems that scan message contents (text, images, videos, files) for matches against a database of objectionable content before the message is sent to the intended recipient. The objectionable content could be a phrase or keyword. There are two types of client side scanning:

1. **comparison performed on the user's device -** The user's device has an app with a full database of 'unique digital fingerprints' of known illegal content. The content that the user is about to encrypt and send in a message is converted to a digital fingerprint and compared to digital fingerprints in the full database. If a match is found, then the message may not be sent, and law enforcement authorities could be notified.
    - There may be significant challenges with maintaining a full database and performing the real-time analysis on a user's device.
2. **comparison performed on a remote server -** The alternative is to transmit the digital fingerprints of a user's content to a server where a comparison with a central database is performed.
    - Last year Apple set out proposals to introduce CSS on its devices but quickly withdrew these citing public backlash.
    - There is currently no available source code to show us what CSS would actually look like and how it would really operate.

CSP - Communications Service Providers offer telecommunications services or some combination of information and media services, content, entertainment and application services over networks, leveraging the network infrastructure as a rich, functional platform.

E2EE - End-to-end encryption is the process of enciphering data so only the sender and intended recipient hold the keys to decrypt the message.[6]

- No third party, even the party providing the communication service, has knowledge of the encryption key.

---

6 https://www.internetsociety.org/issues/encryption/what-is/#:~:text=End%2Dto%2Dend%20encryption%20is,encryption%20that%20you%20can%20use

- It is commonly used to protect both data stored on computer systems (data-at-rest), and data transmitted via computer networks, including the Internet (data-in-transit).
    - **For data-in-transit,** data is generally scrambled using a public key and unscrambled using a private key.
    - **For data-at-rest,** the secret value is typically known only by the data owner.
- End-to-end encryption is the most secure form of encryption that you can use.
- **Exceptional access,** such as **encryption back doors,** refers to some means of allowing law enforcement the ability to lawfully access the content of communications and data in an unencrypted form.
    - However, the consensus among technology experts is that no matter the method, exceptional access makes it easier for other parties, like criminals and other governments, to gain access to secured data.

ECHR - The European Convention on Human Rights protects the rights of people in member states of The Council of Europe which was founded after the Second World War to protect human rights and the rule of law, and to promote democracy. Originally proposed by Winston Churchill and drafted mainly by British lawyers, the Convention was based on the United Nations' Universal Declaration of Human Rights. It was signed in Rome in 1950 and came into force in 1953.[7] The only states on the European continent who are not parties to the treaty are the dictatorships of Belarus and Russia.

IPA - The Investigatory Powers Act 2016 allows the intelligence services and other government agencies to access the private communications and personal information of UK citizens irrespective of whether there is any evidence of wrongdoing. All applications to exercise bulk surveillance powers require a warrant from the secretary of state, who must be satisfied the request is necessary and proportionate. Use of the bulk surveillance powers is also subject to approval by an independent judicial commissioner.

[7] https://www.equalityhumanrights.com/en/what-european-convention-human-rights

SUMMARY OF THE LEGAL ADVICE

Matthew Ryder KC's legal opinion considers existing precedents under international and domestic law that the Online Safety Bill engages with. He has found there is a significant amount of work to be undertaken by Parliament if the legislation is to comply with UK human rights protections and not undermine long-standing protections against state intrusion into the private lives of UK citizens. The report raises serious concerns that Section 104 notices are not a proportionate measure to the issues the notices seek to address, and therefore unnecessary in a democratic society. The key points in the legal advice are as follows:

1. **Surveillance sanctioned under Section 104 Notices would constitute a serious interference with internet / communication service users' rights to a private life and to freedom of expression.**
    - The case law of the European Court of Human Rights recognises the role of anonymity in "promoting the free flow of ideas and information in an important manner" including by protecting people from reprisals for their exercise of freedom of expression (Delfi AS v Estonia [2015] EMLR 26, [147] and [149])
    - The freedom to "hold opinions and to receive and impart information and ideas without interference by public authority" protects not only the content of information but also the means by which it is communicated (Ahmet Yildirim v Turkey (2012) application no. 3111/10, [50])

2. **Under a Section 104 notice, the content of users' communications would be scrutinised on a generalised ongoing basis and in circumstances in which they are not suspected of any wrongdoing.**
    - mandating general, indiscriminate retention of this kind of information will be disproportionate (for the purposes of the rights to privacy and freedom of expression) unless the state is "confronted with a serious threat to national security which is shown to be genuine and present or foreseeable" (and other criteria are satisfied) (La Quadrature; Ekimdzhiev v Bulgaria (2022) 75 EHRR 8, [138] – [139], [168])

3. **Proposed interferences with the rights of service users are unlikely to be in accordance with the law because there is no provision for independent authorisation or oversight of surveillance and no clarity as to how safeguards would be applied in practice.**
    - There must be independent oversight at each stage of the process to assess the necessity and proportionality of the measures being taken. Bulk surveillance "should be subject to independent authorisation at the outset," and there must also be supervision and independent review after surveillance is undertaken or it would not be in accordance with the law. (Big Brother Watch & ors v UK (2022) 74 EHRR 17, [450])

4. **The ECtHR has set out the minimum legal safeguards needed when a state seeks to carry out bulk surveillance which do not appear in the Bill, namely the:**
    - (1) grounds upon which bulk interception might be authorised;
    - (2) circumstances in which an individual's communications might be intercepted;
    - (3) limits on the duration of interception;
    - (4) procedure to be followed for examining, using and storing the data obtained;
    - (5) precautions to be taken when communicating the data to other parties,
    - (6) circumstances in which intercepted data may or must be erased / destroyed.

5. **There are no enhanced safeguards to protect journalistic sources and/or confidential journalistic material.**
    - Material that contains confidential journalistic information (or may identify a source), its "continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination is "justified by an overriding requirement in the public interest"

OUR WIDER SECURITY CONCERNS

Index on Censorship strongly believes that **mass surveillance is not the answer** to effective content moderation regulation under the Online Safety Bill. The Section 104 Notice is perhaps chief amongst the suite of poorly-conceived powers that raises concerns for us on the protection of the right to free speech. Under the clause, Ofcom will have a new power to issue notices to a technology platform requiring it to identify and take down terrorism content communicated "publicly"; or Child Sex Exploitation and Abuse ("CSEA") content, communicated "publicly or privately". Failure to comply with the notice could result in a range of severe penalties. We believe the current draft of the Online Safety Bill will create insecurity because:

A. **Section 104 Notices open the door to the widespread use of Surveillance Technology** because companies can be compelled to monitor every form of communication between users in order to flag whether CSEA or terrorism material is contained within it. Ofcom will have the power to issue these notices on the most secure private messaging platforms such as WhatsApp, Signal and Telegram which have over 43 million active UK users. The platforms cannot currently access users' content as it is end-to-end encrypted, whereas Section 104 notices include the power to compel client and server side scanning which will critically undermine end-to-end encryption on these platforms. Any solution to monitor content is a de facto ban on end-to-end encryption.

B. **Technology companies will need to indiscriminately analyse private messages currently protected by end-to-end encryption.** Companies in scope will be forced to monitor and analyse private communications en masse to avoid the risk of facing fines of up to £18 million or 10% of a company's global annual turnover – whichever is higher. This inevitably will include the choice of whether to comply with back-door requests and give just UK users less protection for their private messages, or to pull out of the UK altogether if the requirements are incompatible with companies' own red lines on encryption technology and the services they provide.

C. **Section 104 notices cover a much wider range of content than the types of surveillance possible under the Investigatory Powers Act 2016.** Matthew Ryder KC's opinion is clear that the power to monitor citizens' content under the Online Safety

Bill is akin to those available to spy agencies such as GCHQ but even spies must, under existing laws, abide by strict legal safeguards and are subject to retrospective compliance monitoring. Surveillance can only be authorised under the powers contained in the IPA if it is both 'proportionate' and 'necessary'. Surveillance has to be in the interests of national security. Bulk surveillance powers under the IPA cannot be used solely for the prevention and detection of serious crime between UK users, there must be some element of national security engaged. Section 104 notices, on the other hand, would compel algorithms to bulk surveil the entire UK population's private communications without any of the careful legal safeguards that have been developed over many years to balance the right to privacy and the issue of national security.

D. **We believe the reliance on algorithms will make users less safe and overwhelm authorities with false flags**. The Bill concedes on the false flag problem by ensuring that terrorism content identified through CSS would not even need to be reported, beyond existing limited legal requirements (contained in other legislation). It would be better if illegal content moderation was carried out in a more targeted way with reasonable suspicion rather than blanket surveillance being the basis of heightened regulatory powers. Instead of making people safer, the surveillance measures may add significant problems to law enforcement taking action against offenders. Algorithms have no regard for context and could flag a perfectly innocent Whatsapp video call between partners whilst nappy-changing their baby or of a parent seeking medical advice about their child's genitals.[8]

E. **The Bill pretends that Section 104 Notices, which impose the mass screening of private communications, do not amount to mass surveillance and therefore do not require the current level of legal safeguards.** There is no provision for an independent oversight (such as by a court to ensure the use of surveillance is necessary and proportionate) of the use of Section 104 Notices even though it may require private bodies – at the behest of Ofcom – to carry out mass state surveillance of millions of user's communications[9]. Whilst there is more needed to address CSEA material online,

[8] https://www.theverge.com/2022/8/21/23315513/google-photos-csam-scanning-account-deletion-investigation
[9] https://www.messengerpeople.com/global-messenger-usage-statistics/#GreatBritain

we do not believe mass surveillance that is absent of any reasonable suspicion is necessary in a democracy. The bill fundamentally undermines the right not to have one's property seized or searched other than by authority of law as there is no process for lawful authorisation for the search for information on a user's device.

F. **Undermining global standards on the privacy of direct messaging is also particularly dangerous for LGBTQ+ individuals and other minorities who are targeted by autocratic governments** and rely on online communication for support and to express themselves. As a global watchdog on freedom of expression, we are concerned that the Bill will lead to a deterioration of E2EE communication services globally. Without encryption, millions of people may be put at risk such as journalists, their sources, and political dissidents across the world, for whom encryption is essential. Recent initiatives like Meta's to increase online security[10] by offering users end-to-end encryption for direct messaging in Russia to protect them from an authoritarian government during wartime demonstrates the current need for security in online spaces.

UKRAINE

- End-to-end encryption acts as a lifeline for people in conflict zones around the world
- Millions of Ukrainians have downloaded end-to-end encrypted apps since the beginning of the Russian invasion to speak to friends and family undetected.
- Encryption is also essential to allow journalists to report information out of Ukraine, and be broadcast around the world.
- For those inside Russia protesting against the war and working underground to help disseminate real news about the invasion to Russian citizens, encryption is essential to avoid imprisonment, torture and even death.

G. **The Bill is vague on how communications might be "identified" by a technology platform as terrorism and CSEA.** There is a lack of clarity as to what the difference between a private or public communication means and relevant content is defined with reference to a wide range of offences but most of these cannot be committed through

[10] https://about.fb.com/news/2022/08/testing-end-to-end-encrypted-backups-and-more-on-messenger/

communicating image/text/audio/video material alone meaning platforms will be required to draw inferences from a user's state of mind with little to no basis in which to do so.

H. **Exposing encryption creates insecurities** - the Bill and the latest amendments proposed by the Secretary of State for DCMS in the last few months, set up technology companies to be forced to use unprecedented state-mandated Surveillance Technology known as Client Side Scanning ('CSS'). Companies will need to monitor private communications in order to avoid large fines, even in circumstances in which users are not suspected of any wrongdoing.

Research shows using of Surveillance Technology breaks end-to-end encryption

- Any attempt to require technology companies to undermine their implementation of end-to-end encryption would have far-reaching implications for the safety and security of online communications.[11]
- Tech and internet security experts agree that the use of CSS opens up a Pandora's box of potential information and cyber security issues[12]
- Any CSS model that affirmatively or negatively reports to a non-participant regarding the nature of content is revealing at least one bit of information and therefore breaking end to end encryption[13].
- Technologists predict that current CSS systems do not detect the majority of CSEA material (in video format) as they are so far only capable of accurately scanning text and static images[14]

[11] *Bugs in our Pockets: The Risks of Client-Side Scanning* https://regmedia.co.uk/2021/10/14/key_risks_paper.pdf

[12] https://www.computerweekly.com/news/252508198/Apple-scheme-to-detect-child-abuse-creates-serious-privacy-and-security-risks-say-scientists

[13] https://cdt.org/insights/to-the-uk-an-encrypted-system-that-detects-content-isnt-end-to-end-encrypted/

[14] *Bugs in our Pockets: The Risks of Client-Side Scanning* https://regmedia.co.uk/2021/10/14/key_risks_paper.pdf

RE: THE ONLINE SAFETY BILL:
HUMAN RIGHTS IMPLICATIONS
OF CLIENT-SIDE SCANNING

LEGAL OPINION

INTRODUCTION AND SUMMARY OF ADVICE

1. We are asked to advise the Index on Censorship and 89up on whether certain provisions of the Online Safety Bill ("**OLSB**")[1] would be compatible with the European Convention on Human Rights ("**the ECHR**").

2. Under Clause 104 of the Bill, OFCOM[2] will have a new power to issue notices to a communications service provider ("**CSP**") requiring it to identify and take down terrorism content communicated "publicly" by means of its service; or Child Sex Exploitation and Abuse ("**CSEA**") content, communicated "publicly or privately" by means of its service. Failure to comply with the notice could result in a range of severe regulatory penalties.

3. A key concern about this new power is that "**104 Notices**" may mandate CSPs to change how their services function. This may include implementing Client-Side Scanning ("**CSS**"), whereby CSPs scan users' communications for particular content or undermining end-to-end encryption to make private communications readable. Accordingly, the power to force CSPs to comply with 104 Notices has significant implications for users' right to private and family life, under Article 8 of the ECHR, and their right to freedom of expression, under Article 10 of the ECHR.

1 At the time of writing, in October 2022, the OLSB is at the report stage in the Commons, it has yet to be considered by the House of Lords.
2 The Office of Communications, the Government-approved regulatory and competition authority for the broadcasting, telecommunications and postal industries of the UK.

4. In summary, our advice highlights a number of concerns:

a) The power granted to OFCOM under Clause 104 ostensibly permits the state to compel CSPs to carry out surveillance of the content of communications on a generalised and widespread basis.

b) In order to be lawful Clause 104 *and* 104 Notices issued pursuant to it, requiring mass[3] surveillance of communications, would need to be accompanied by rigorous safeguards to be "in accordance with the law" and "prescribed by law", as is required by Article 8 and 10 the ECHR respectively, and to comply with English law.

- The failure to have any form of independent prior authorisation or independent *ex post facto* oversight for such a sweeping power is likely to breach Articles 8 and 10 of the ECHR.

- Other safeguards exist in Clause 105 of the OLSB, but whether those additional safeguards will be sufficient will depend on how they are applied in practice. There is currently no indication as to how OFCOM will apply those safeguards and limit the scope of 104 Notices. For example, Clause 105(h) alludes to Article 10 of the ECHR, by requiring appropriate consideration to be given to interference with the right to freedom of expression. But there is no specific provision ensuring the adequate protection of journalistic sources, which will need to be provided in order to prevent a breach of Article 10.

- Further, some of the legal definitions in or attaching to Clause 104, including the definitions of (i) the content that can be targeted under 104 Notices and (ii) whether a communication is private or public (as set out

[3] We have used the term "mass" surveillance, rather than the term "bulk" surveillance because the latter is now a recognised legal term, meeting a particular definition within the Investigatory Powers Act 2016. In contrast, the seeping surveillance potentially imposed by 104 Notices is even broader and less constrained than the bulk surveillance powers that exist under the IPA.

in Clause 188) are currently too vague for the powers dependent on those definitions to have sufficient certainty and foreseeability.

- Interferences with Articles 8 and 10 of the ECHR arising from surveillance under Clause 104 would also need to be necessary in a democratic society, which encompasses a requirement that it be proportionate to the aim pursued. We have considerable doubt that the aims pursued are sufficient to justify the serious interference with privacy and freedom of expression of very large numbers of people. Further, given the existing powers of intrusive surveillance under the Investigatory Powers Act 2016 ("**IPA**"), including both targeted and bulk forms of interception and equipment interference, there may be other less intrusive means available for pursuing those aims. It is therefore doubtful that Clause 104 can properly be regarded as necessary in a democratic society.

c) Even if the lawfulness of Clause 104 could be theoretically established in general terms, in order to be used lawfully specific 104 Notices would have to be issued only in circumstances where it was necessary and proportionate to do so. In our opinion 104 Notices mandating mass surveillance of millions of lawful users would require very substantial justification, and there would be real difficulties in establishing such justification:

- Any attempt to require CSPs to undermine their implementation of end-to-end encryption generally, would have far-reaching implications for the safety and security of all global online communications. We are unable to envisage circumstances where such a destructive step in the security of global online communications for billions of users could be justified. The real and far-reaching dangers of public authorities requiring CSPs to undermine end-to-end encryption are familiar and have been exhaustively discussed, for many years, in a variety of contexts and cases. For that reason, we have not repeated those arguments in this advice. Furthermore, there is no express indication that such a draconian step is contemplated by giving OFCOM the power to issue 104 Notices. We have therefore focused this advice on the potential introduction of CSS by 104 Notices.

- Any attempt to require all CSPs to implement CSS for all communications by all users of eligible services may be potentially achievable but is so unlikely to achieve its purported aim, and so unlikely to provide a functional solution for the harm it is intended to address, as to be a disproportionate step in practice. For example, it is difficult to see how offending content could be identified for all communications on the platform unless the content of all communications was read in a way that not only examined the content of each communication but was able to place it in context. That level of granular examination would either be unworkably intrusive of communications by all users or necessarily targeted and therefore limited to those users whose communications could be examined under less intrusive powers with more structured safeguards, such as those contained under the IPA.

5. For the above reasons, which are developed below, we conclude:

   a) Surveillance pursuant to 104 Notices would constitute a serious interference with users' rights to a private and family life and to freedom of expression under the ECHR. The exercise of powers under Clause 104 may also engage the ECHR rights of CSPs.

   b) Interferences with the rights of service users arising from surveillance under 104 Notices are unlikely to be in accordance with the law/prescribed by law for the purposes of Articles 8 and 10 of the ECHR. That is primarily because there is no requirement for any independent authorisation or oversight of surveillance under Clause 104; there is currently no clarity as to how purported safeguards would be applied in practice; and there are serious problems with the definition of the content that would be targeted for identification and blocking.

c) It is also doubtful that interferences with those rights arising from the imposition of 104 Notices would be proportionate and thus necessary in a democratic society. Those concerns would arise both in relation to Clause 104 in the abstract and to interferences arising from the issuing of a specific notice to CSPs under Clause 104.

6. In our view, the amendments to Clause 104 tabled by the Secretary of State on 26 October 2022 would not materially change this analysis.

BACKGROUND

RELEVANT PROVISIONS IN THE ONLINE SAFETY BILL

7. This opinion is concerned primarily with provisions in the OLSB which may empower the regulator, OFCOM, to compel online CSPs to scan users' communications for particular content. Those provisions exist alongside requirements to disclose certain material to the National Crime Agency ("**NCA**"), and regulatory powers (including sanctions) to force service providers to comply with these obligations.

Notices requiring service providers to "deal with" terrorism and CSEA content

8. Clause 104[4] of the OLSB is entitled "*Notices to deal with terrorism content or CSEA content (or both)".* It appears in Part 7 of the Bill which concerns "*OFCOM's powers and duties in relation to regulated services*". It empowers OFCOM to give notices requiring the providers of "regulated user-to-user services" to use what is referred to as "accredited technology" to (a) identify and (b) take down[5] particular content that is communicated through the service publicly (in the case of terrorism content) or publicly or privately[6] (in the case of CSEA content).[7]

[4] The references contained in this advice are to the OLSB as amended by the Public Bill Committee; this version of the Bill is dated 28 June 2022. Shortly before we finalised this advice the Secretary of State tabled an amendment to Clause 104, which would see the existing clause replaced in its entirety. The main changes are set out below.
[5] Meaning removed from a service or permanently hidden so users cannot reencounter it (c.192(1)).
[6] Whether content is considered to be communicated publicly or privately depends on a wide range of factors, see c.188(2)(3).
[7] There is an equivalent provision concerning so-called "search services" but that is not the focus of this advice.

Content would include images, words and sounds. The proposed amendment to Clause 104 would expand the potential scope of 104 Notices to include requiring CSPs to use accredited technology "*to prevent individuals from encountering"* terrorism content and CSEA. The amendment appears to contemplate that OFCOM may require CSPs to use accredited technology to block content as an alternative to taking it down.

9. The OLSB does not name the specific accredited technologies which OFCOM may mandate CSPs to use. The accreditation of technologies will be done by OFCOM or its appointees on the basis of minimum standards of accuracy – laid down by the Secretary of State – for detecting CSEA or terrorism content (c.106(9)(10)). The proposed amendment would empower OFCOM to require CSPs to "*to use their best endeavours to develop or source technology for use on or in relation to the service*" which achieves the purposes set out above. It seems that this may be in addition or in the alternative to using accredited technologies. While we do not know which technologies OFCOM will accredit and include within 104 Notices, or which technologies CSPs themselves develop or source, for the reasons we explain below CSS is likely to be the primary technology whose use is mandated. Service providers may comply with 104 Notices by way of accredited technology alone or in combination with human moderators (c.104(5)).

10. Clause 104 Notices could impose requirements on a CSP for up to 3 years (c.106(6)). The Bill is silent on whether 104 Notices would or could be made public. There is no express prohibition on a service provider disclosing the fact that they are the subject of a Notice[8] but this could, in principle, be imposed through statutory guidance or on the face of a Notice. A failure to comply with a Notice could lead to regulatory action including the imposition of substantial fines and the blocking of services.

[8] Cf. the position in relation to communications data retention notices issued under Part 4 of the Investigatory Powers Act 2016; section 95(2) of that Act expressly forbids the disclosure of the existence of such notices or their content.

The content targeted by Clause 104

11. Clause 104 of the OLSB, and 104 Notices issued pursuant to it, is aimed at preventing the circulation online of what the Bill calls “terrorism content” and “CSEA content”. These terms are defined as content “which amounts to” to one or more a wide range of offences relating to (a) terrorism (set out in Schedule 5) and (b) child sexual exploitation and abuse (set out in Schedule 6). The offences in the schedules are *not* confined to offences committed by communicating particular information. Indeed, most of these offences do not include this as one of their constituent elements. That being so, it is not clear how content on/communicated through services could “amount to” (which appears to mean the commission of) these offences. For example, neither the sending of a communication, nor its content, could amount to the “possession of money or property for terrorist purposes” or the “laundering of terrorist property”, just two of the offences under the Terrorism Act 2000 which are included within Schedule 5 to the OLSB.

12. The requirement that the content of a communication must amount to an offence is significant. It indicates that 104 Notices are not considered appropriate merely for intelligence gathering or general monitoring, but apply only to identifying and removing content that “amounts to” evidence of the specific criminal offences being committed. This is important when considering whether existing, more targeted powers for identifying the commission of offences should be used instead.

13. In order to assess whether particular information is capable of amounting to (or being evidence of) particular offences there would be a need to analyse communications in some detail. It is difficult to see how this could be achieved in practice, particularly if this were to be done through technology alone (as appears to be contemplated by the Bill). Applying key words or selectors to communications would be unlikely to be sufficient to assess whether, for example, particular messages suggest that the sender is engaged in the “encouragement of terrorism” or is “arranging a meeting supportive of a proscribed organisation” (two of the offences in paras 1 and 2 of Sch 5 to the OLSB).

Subjects of Notices

14. OFCOM would issue 104 Notices to "regulated user-to-user services". The OLSB defines "user-to-user services" in expansive terms to include "*an internet service by means of which content that is generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service may be encountered by another user or other users of the service*" (c.2(1)). A service is "regulated" if (a) it has a significant number of UK users, UK users form a target market, or if the service is capable of being used by people in the UK *and* there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK ; and (b) it is not exempted under Schedule 1 (c.3). Exempt services (which may be amended by secondary legislation) include email only services, SMS/MMS[9] only services; and live aural communications (Sch 1, paras 2-3 to the OLSB).

15. CSPs to whom 104 Notices may be given would, therefore, include providers of internet-based communications applications and social media platforms. That would likely include services such as WhatsApp, Messenger, Telegram, Signal, Instagram, TikTok and Facebook. Having regard to the apparent aims of the OLSB and the 104 Notices in particular – it seems likely that OFCOM would issue 104 Notices to all relevant CSPs.

Circumstances in which 104 Notices could be issued

16. OFCOM could only issue a 104 Notice to a CSP if it considers it is necessary and proportionate to do so (c.104(1)). When making this assessment, mandatory considerations for OFCOM are set out in c.105(1). These include: the kind of service; its functionalities and user base; the prevalence of the relevant content on the service; the level of risk of harm to presented by the relevant content; the extent to which the use of the technology mandated by a Notice would/might interfere with users' freedom of expression; the level of risk that the use of the technology would result in a breach of privacy or data protection law; and whether less intrusive measures would be likely to achieve a significant reduction in the relevant content.

[9] These are essentially messages sent between two telephone numbers (c.49(12)).

OFCOM will be required to produce statutory guidance on how it shall exercise its powers relating to the giving of 104 Notices (c.108).[10] At present, there is no indication as to how OFCOM will apply those safeguards or constrain the parameters of the power granted to it under Clause 104.

17. It is notable that 104 Notices can only be issued in relation to terrorist content that is "communicated publicly" (c.104(2)(a)), while 104 Notices may be issued in relation to CSEA content communicated publicly or privately. Yet the OLSB contains no definition as to what constitutes a public communication, as opposed to a private communication. Instead, Clause 188 merely lists a range of factors that OFCOM must consider in determining whether content is communicated publicly or privately (c.188(2)). These include: the number of persons in the UK who are able to access the content by means of the service; any restrictions on who may access the content by means of the service; and the ease with which the content may be forwarded to or shared with users of the service other than those who originally encounter it. In the absence, so far, of any guidance as to how OFCOM will take into account those factors, the distinction between a private and a public communication risks being both unclear and arbitrary.

Obligations in relation to content identified

18. Beyond "taking down" (or under the proposed amendment, preventing users from "encountering") the relevant content, Part 7 of the OLSB does not specify what providers should do with content they identify. However, Part 4 places service providers under a range of reporting duties. This includes an obligation to report CSEA content to the NCA. Service providers are required to operate services using "*systems and processes which secure (so far as possible)*" that they report all "detected"[11] and "unreported" CSEA content. Non-UK providers are required to do this in respect of UK-linked CSEA content (c.59(1)(2)).[12]

[10] There is no draft guidance or any indication of what it may contain.

[11] CSEA content is "detected" by a provider when the provider becomes aware of the content, whether by means of the provider's systems or processes or as a result of another person alerting the provider (c.63(4)).

Detected content would, it appears, include content identified on the basis of the use of accredited technology pursuant to a Notice. Accordingly, the OLSB not only creates a power to mandate service providers to identify CSEA content but also to report this to law enforcement.

19. There is no equivalent obligation in relation to terrorism content, but it is unclear as to why. If this is because analysing the detail and content of conversations and discussions in relation to potential terrorist content would be considered too onerous, or too difficult to apply in practice, the same difficulties would apply to CSEA content (other than digital material that can be automatically identified by hash markers, such as images already known to the authorities). Without further explanation this distinction suggests a fundamental inconsistency and misconceived practical distinction that may make 104 Notices unworkable in practice.

CLIENT-SIDE SCANNING

20. CSS is the use of software to screen communications sent (or proposed to be sent) from a device and/or through an app for the presence of information whose communication (or attempted communication) the operator wishes to identify, prevent and/or report. It functions through algorithmic analysis of information (in picture or text form) generated by a user to ascertain whether it matches, or closely resembles, either (i) information on a database or (ii) information of a kind that the system has been "trained" and/or "learns" to recognise.

21. Scanning of communications can be done in two broad ways.[13] The system could be "client side" – i.e., "on" communications devices, such as smartphones, either as part of the operating system or, more likely, within a communications app.

[12] Content is "UK-linked" if a service provider has evidence of a link between the content and the United Kingdom, based on, inter alia, the place where the content was published, generated, uploaded or shared; the nationality of a person suspected of committing the related offence; the location of a person suspected of committing the related offence; or the location of a child who is a suspected victim of the related offence"(c.63(6)).

[13] For further discussion see, for example, Adelson et al., "Bugs in our Pockets: the Risks of Client-Side-Scanning" (October 2021).

Alternatively, the system may be located on the CSP's server – with scanning performed when communications are transmitted through a server. Where scanning identifies matches or likely matches, systems can be configured to, for example, block the communication of the material, to flag it for human review and/ or transmit it directly to a third party such as law enforcement. Scanning will work only if the information being scanned is not encrypted.[14] It therefore has to be implemented on the "client side" – on device – before or after information is encrypted / decrypted for transmission by a system which uses end-to-end encryption.

22. Clause 104 does not refer to CSS (or any technology) by name. It mentions only "accredited technology". However, the practical implementation of 104 Notices requiring the identification, removal and/or blocking of content leads almost inevitably to the concern that this power will be used by OFCOM to mandate CSPs using some form of CSS. The Bill notes that the accredited technology referred to c.104 is a form of "content moderation technology", meaning "*technology such as algorithms keyword matching image matching or image classification which analyses relevant content*" (c.187(2)(11). This description corresponds with CSS. In the summer of 2022 two senior GCHQ officials published an article in which they endorsed CSS as a potential solution to the problem of CSEA content being transmitted on encrypted platforms.[15] These comments were made against the backdrop of the ongoing debate about the OLSB.

23. As noted above, the proposed amendment to Clause 104 envisages that OFCOM could require CSPs to "use best endeavours" to develop or source their own technology to achieve the same purposes as accredited technology. It seems likely that any such solution would be CSS or something akin to it. We think it is highly unlikely that CSPs would instead, for example, attempt to remove all end-

[14] It is, of course, possible to read communications in circumstances where encrypted communications can be decrypted. But this would require a backdoor' into breaking established forms of decryption, such as altering the random number generator in an encryption ratchet system. Creating such a weakness would then undermine encryption security for all communications on that platform.

[15] I. Levy and C. Robinson, "Thoughts on Child Safety on Commodity Platforms" (July 2022).

to-end encryption on their services. Doing so would not remove the need for them to analyse the content of communications to identify relevant content. More importantly, however, this would fatally compromise security for their users and on their platforms, almost certainly causing many users to switch to other services.

Risks identified in relation to CSS

24. Communications security experts have produced extensive literature dealing with the weaknesses of and security risks that may arise from CSS.[16] In summary, these arise in three areas. First, problems of accuracy can occur, leading to high rates of false positives and false negatives. This is generally affected by all or a combination of the scanning algorithm, the content of the database used (if applicable), and problems with any training data (where used). Second, third parties may be able to manipulate CSS systems to alter or add to the types of information that are flagged by the system; that could do anything from increasing the rate of false negatives to causing the system to identify material which is entirely lawful. Finally, putting CSS systems on devices creates weaknesses and vulnerabilities in software and OS structures and may create opportunities for unauthorised actors to hack into these systems to, for example, obtain information or install malware.

DISCUSSION AND ADVICE

25. If it is used as anticipated, Clause 104 introduces an entirely new way of monitoring communications, by empowering a public authority to require CSPs to monitor the **content** of potentially all their users' communications at all times for a very broad range of criminal offences (albeit under two headings – terrorism and CSEA). This goes further than surveillance of content where the communication of the content itself necessarily constitutes a criminal offence (e.g., the communication of CSEA images). It includes circumstances where the nature and context of conversations by users will need to be analysed in detail to determine the commission of offences.

[16] See for example: Adelson et al., pp12-14, 21-26.

26. If OFCOM were to compel the use of CSS to perform such analysis, this would, in our view, amount to generalised, state-mandated mass surveillance of communications by the private sector.[17] To borrow the words of the Court of Justice of the EU ("**CJEU**"), this type of surveillance is "*likely to generate in the minds of service users the feeling that their private lives are the subject of constant surveillance*" (C-293/12 *Digital Rights Ireland Ltd v Minister for Communications Marine and Natural Resources* [2015] QB 127, [37]).

27. In light of the above, Clause 104 has generated concerns in three main ways:

    a) the prospect of all communications on regulated user services being monitored for their content;
    b) the possibility that 104 Notices will require service providers using end-to-end encryption to undermine encryption, with serious wider consequences; and
    c) the relationship with and comparison between monitoring pursuant to 104 Notices and existing surveillance powers.

    These points are relevant to the broader assessment of the lawfulness of the proposed power.

SCOPE OF THE CLAUSE 104 POWER

28. There is an inherent tension in the need to ensure that Clause 104 achieves its purpose, while ensuring that 104 Notices are proportionately targeted and restrained in their use. In particular, it is difficult to see how the apparent aims of Clause 104 – ensuring that no CSPs allow particular content to be communicated on their services at any time - would be accomplished if 104 Notices were only issued to a limited number of platforms, particularly if 104 Notices were made public. If so, users could simply avoid having their communications monitored by switching to a different service. But if 104 Notices were issued across all eligible platforms, this would mean that the content of a almost all internet-based

[17] In our view, the same would be true of a 104 Notice mandating a CSP to use their best endeavours to develop or source technology to achieve aims set out in Clause 104.

communications by millions of people – including the details of their personal conversations - would be constantly surveilled by service providers. Whether this happens will, of course, depend on how OFCOM exercises its power to issue 104 Notices, but the inherent tension between the apparent aim, and the need for proportionate use is self-evident.

29. It is not just the quantity of communications that would pose a problem, but the detailed intrusive nature of the surveillance that would need to take place on each communication. As we explain above, we have considerable difficulty seeing how material falling into the definitions of "terrorism content" and even CSEA could be identified and taken down without the content of vast amounts of communications also being analysed by humans. But even if we are wrong about that, the content of all communications on relevant platforms would be scrutinised by software using what would necessarily include very generalised selectors or key words. Communications would therefore still need to be monitored by the CSP and would not remain confidential to the parties to the communication.

THE RELATIONSHIP WITH END-TO-END ENCRYPTION

30. End-to-end encryption is now standard on most communications platforms, including most, if not all, the services which may be the subject of 104 Notices. This protects data while it is in transit and is an essential part of protecting the privacy of correspondence and safeguarding anonymity online. Not only does end-to-end encryption protect privacy but, as the courts and international special mandate holders have recognised, it also promotes the exercise of other rights.[18] The case law of the European Court of Human Rights ("**ECtHR**") recognises the role of anonymity in "*promoting the free flow of ideas and information in an important manner*" including by protecting people from reprisals for their exercise of freedom of expression (*Delfi AS v Estonia* [2015] EMLR 26, [147] and [149]).

[18] For example, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* A/HRC/29/32 (May 2015), paras 16 – 24.

31. Third party monitoring of the content of communications risks undermining one of the fundamental objectives of end-to-end encryption, if to do so requires creating a "backdoor" that enables the decryption of communications by anyone other than the parties to that communication. For reasons outlined in the following paragraph, we anticipate that the monitoring of communications content can and would be done through mandating CSS rather than through mandating the breaking of established encryption protocols. To require the latter over the former would be disproportionate. If 104 Notices were to require service providers to compromise encryption protocols that would give rise to fundamental concerns as to the security of all online communications for all purposes including commercial transactions. Accordingly, we consider any notice that mandated the breaking of end-to-end encryption would be extremely difficult to justify as proportionate.

32. We will not, however, know definitively whether end-to-end encryption will be the subject of 104 Notices, until such notices are issued in practice. For substantially the same reasons, it seems unlikely that, if mandated by OFCOM to develop or source their own technology to identify, take down or block content, CSPs would choose to break end-to-end encryption.

33. At this point we anticipate 104 Notices may focus on requiring CSPs to use CSS that monitors communications "on device" either before or after encryption and may therefore be carried out without necessarily undermining existing end-to-end encryption protocols. It should be noted that even CSS may create vulnerabilities on devices or platforms which could lead to end-to-end encryption being weakened or broken. But that is a different proposition from deliberately creating a backdoor that removes end-to-end encryption from otherwise encrypted communications.

34. If, as we anticipate, CSS in some form is the accredited technology that OFCOM elects to mandate, concerns about 104 Notices necessarily requiring the breaking of encryption protocols may be overstated.[19] For that reason we consider the key human rights concerns arising from Clause 104 to be the mass surveillance of communications on device, similar to the existing use of bulk surveillance powers.

COMPARISON WITH EXISTING SURVEILLANCE POWERS

35. The IPA contains a range of powers enabling the intelligence services and law enforcement bodies to obtain the content of communications. These include targeted interception and equipment interference warrants. Those are more focused than the sweeping surveillance contemplated under Clause 104 because they must comply with the specific defined criteria for targeting set out in the IPA.[20] CSS that may be mandated by 104 Notices is, therefore, less analogous to targeted warrantry under the IPA but shares important features of two "bulk" surveillance powers under Part 6 of the IPA: (a) bulk interception; and (b) bulk equipment interference. For the reasons we explain below, this comparison is relevant to the assessment of the human rights compliance of Clause 104 because the jurisprudence establishes minimum safeguards which are required in order for these existing bulk surveillance powers to be lawful.

36. "Bulk" interception is carried out under the statutory powers contained in Chapter 1 of Part 6 of the IPA. It can authorise the interception of overseas-related communications (meaning that one party to the communications is outside the British islands) that are being transmitted and the subsequent automated analysis and human examination of the content of those communications on the basis of "selectors" relating to topics of interest.

[19] Clause 104 also shares similarities with the power under the IPA (s 253) to give telecommunications operators so-called "technical capability notices" for the purposes of "*securing that the operator has the capability to provide any assistance which the operator may be required to provide in relation to*" a warrant for e.g., interception or equipment interference under the IPA. Public concerns that this may lead to notices requiring the breaking of end-to-end encryption do not appear to have materialised.

[20] For example, s17 of IPA requires Targeted Interception Warrants to relate to: a particular person or organisation; a single set of premises; a group of persons who share a common purpose or who carry on a particular activity; a single investigation or operation; testing or training activities.

37. Bulk equipment interference is carried out under Chapter 3 of Part 6 of the IPA. It entails interference with communications equipment (and associated equipment) for the purposes of, among other things, obtaining overseas-related communications, equipment data or any other information. This can include obtaining the content of communications, but only if such communications are stored on the device, not if the communications are being transmitted. Under the IPA, both of these types of bulk surveillance can only be used by the intelligence services and they can only be used where it is necessary in the interests of national security (alone), or national security *and* preventing or detecting serious crime, or in the interests of the economic well-being of the UK provided that those interests are relevant to national security.

38. Mandating a ubiquitous form of CSS by a CSP would resemble bulk interception and bulk equipment interference in that it would involve the screening of the content of communications of large numbers of people (in the case of CSS, everyone using a particular communications service and, in the case of bulk interception, everyone whose communication passes along a particular bearer) in circumstances in which there is no suspicion that any given subject of the surveillance has engaged in wrongdoing. In both cases, all communications would be scrutinised for the presence of particular content.

39. While the modalities of mass surveillance under the IPA bulk powers and mass surveillance under 104 Notices would be different, the privacy implications for communications service users are broadly similar. Unlike the IPA's bulk powers, however, Clause 104 covers/targets a much wider range of content. It potentially permits the use of much broader selectors when communications are monitored for relevant content. Further, as we explain below, Clause 104 and Notices issued under that provision are not accompanied by equivalent safeguards.[21]

[21] It is notable that the "bulk" surveillance powers under the IPA were the subject of intense debate, careful scrutiny, a specific analysis by David Anderson QC prior to their enactment resulting in a nuanced framework that is subject to limitations and judicial oversight. There has been little equivalent debate as to the appropriateness of giving OFCOM the power to mandate potentially even broader "mass" surveillance powers.

THE HUMAN RIGHTS FRAMEWORK

40. We have examined the human rights compliance of Clause 104 / CSS primarily with reference to the ECHR and, to lesser extent, common law fundamental rights. We have not considered the position in respect of the UK's international law obligations under the International ECHR on Civil and Political Rights as a discrete issue because we consider the analysis to be substantially the same as under the ECHR.[22]

Relevant substantive rights

41. The human rights concerns arising from Clause 104 (and mandatory CSS generally) relate primarily to the users of communications services that would be the subject of 104 Notices. The right most obviously engaged is the right to a private and family life under Article 8(1) of the ECHR, which includes a right to respect for one's correspondence. CSS involves generalised surveillance of correspondence by a person who is not party to it and their accessing of the content of communications that is private and confidential. Article 8 is engaged regardless of whether a human looks at a communication and regardless of any further use that is made of that data.[23] Any further examination, use or storage of information identified through CSS constitutes additional, discrete interferences with Article 8 rights.

42. The other fundamental right of users which is in play is the right to freedom of expression under Article 10 of the ECHR. That includes the freedom to "*hold opinions and to receive and impart information and ideas without interference by public authority*". This right protects not only the content of information but also the means by which it is communicated.[24] The services through which people communicate digitally are essential platforms and forums for the exercise of the right to freedom of expression.[25] Article 10 is relevant in at least three ways.

---

[22] The EU Charter of Fundamental Rights no longer applies in the UK but its case law in relation to the rights to privacy and freedom of expression is of relevance to our analysis.

[23] *Big Brother Watch (BBW) & ors v UK* (2022) 74 EHRR 17; [325] – [331]; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others v Premier ministre* [2021] 1 WLR 4457 ("*La Quadrature"*) [116].

[24] *Ahmet Yildirim v Turkey* (2012) application no. 3111/10, [50].

[25] See for example, *Ahmet Yildirim*, [48] – [49]; *Vladimir Kharitonov v Russia* (2020) application no. 10795/14), [33]; *Delfi* [110].

43. Firstly, communications may be taken down or blocked and that may happen erroneously due to false positive identifications. Second, users of communications platforms may be dissuaded from communicating due to concerns about not being able to do so in confidence and/or being monitored, i.e., the use of CSS may have a "chilling" or "deterrent" effect on their freedom of expression.[26] That effect may be particularly acute in respect of sources who assist the press in public interest journalism or those who provide information to NGOs and human rights defenders.[27]

44. Third, a CSP's *own* ECHR rights may also be engaged. The ECtHR has held that the Article 10 rights of the provider of a blogging platform were engaged by imposing liability for and/or compelling the removal of content from the platform, even though that content was not curated or edited by the service provider (*Tamiz v UK* [2018] EMLR 6, [90]). The Article 10 rights of the providers of a file sharing platform are also, the ECtHR has concluded, engaged by holding them liable for their users' breaches of copyright – that is because they "*put in place the means for others to impart and receive information*" (*Neij & Sunde Kolmisoppi v Sweden* (2013) application no. 40397/12, p.10). We think there is a reasonable argument that the Article 10 rights of service providers would be similarly engaged by the imposition of 104 Notices and associated measures.

Engagement of ECHR rights

45. The mere enactment of a legislative provision that permits communications surveillance, may engage the ECHR rights of all communications service users, even prior to the issuing of specific notices against users.[28] This is particularly the case if the use of that power is kept secret to the extent that users are unable to know whether their communications are being subject to that surveillance power. But even if it were not accepted that the mere existence of powers to mandate

[26] See by analogy: *La Quadrature*, [118] and [173].
[27] The ECtHR has recognised NGOs perform a public watchdog role similar to the press when they draw attention to matters of public interest and should therefore attract similar protections under Article 10 to those afforded to the press (*Magyar Helsinki Bizottsag v Hungary* (2020) 71 EHRR 2, [166]-[167]).
[28] *Weber & Saravia v Germany* (2008) 46 EHRR SE5, [78].

CSS on communications services is sufficient to engage ECHR rights, there is no doubt that the issuing of a 104 Notice to a service provider would engage the rights of the users of that service (and those of the service provider).

46. The fact that the OLSB mandates surveillance by private bodies – rather than directly by the state itself – does not, in our view, prevent the application of human rights protections to the users' communications. The courts have frequently applied human rights law to, for example, legislative measures compelling the collection and retention and disclosure of communications data retention by CSPs,[29] and their collection and retention of personal data in connection with SIM cards.[30] Given the proposed approach to 104 Notices, the surveillance that OFCOM would mandate CSPs to undertake would be carried out at the behest of the state.[31]

47. In any event, the ECHR requires that states secure the rights and freedoms of persons within their jurisdiction. This positive obligation may require action (including legislative, regulatory and law enforcement action) to be taken in respect of relations between individuals. The ECtHR has emphasised that this extends to ensuring that surveillance undertaken by private bodies complies with the ECHR.[32]

ASSESSMENT OF COMPLIANCE WITH HUMAN RIGHTS

Introduction

48. As we explain above, Clause 104 would give rise to significant interferences with both the right to privacy and the right to freedom of expression of relevant communications service users.[33] The content of their communications would be scrutinised on a generalised and ongoing basis in circumstances in which they are not suspected of any wrongdoing. Initial monitoring would be done by

[29] See for example, *R (Davis & Watson) v SSH* [2016] 1 CMLR 13; *La Quadrature*; *Ekimdzhiev v Bulgaria* (2022) 75 EHRR 8.

[30] See for example: *Breyer v Germany* (2020) 71 EHRR 17.

[31] See by analogy *Ekimdzhiev v Bulgaria*, [375].

[32] *Barbulescu v Romania* [2017] IRLR 1032, [108] – [122], and *Lopez Ribalda v Spain* (2020) 71 EHRR 7, [109] – [116] (these were about surveillance of employees by employers).

[33] The analysis is substantially the same under both of these rights, save for certain issues which are specific to Article 10 of the ECHR, as discussed below.

software but, given the scope of the content targeted by Clause 104, we think it is inevitable that there would also be human scrutiny of a substantial number of communications. That markedly increases the extent of the interference.[34]

49. Our assessment of compliance with human rights law focuses on Clause 104. Individual exercises of this power by OFCOM, through issuing 104 Notices, may give rise to specific human rights issues. As may the statutory guidance that will ultimately be promulgated by OFCOM in respect of this power. These are not, however, matters that can be evaluated at this stage. Many of our observations on the human rights implications of Clause 104 apply generally to state mandated CSS.

Article 8(2) ECHR and Article 10(2) ECHR

50. To be justified, and thus lawful, interferences must be "in accordance with the law" (Article 8) or "prescribed by law" (Article 10)[35], in pursuit of a legitimate aim, and necessary in a democratic society. Necessity encompasses a requirement that the interference corresponds to a pressing social and is proportionate to the aim pursued.

<u>In accordance with the law / prescribed by law</u>

51. Interferences will not be in accordance with the law unless they have some basis in domestic law, are accessible and foreseeable[36]. It is the third of these requirements that is of relevance to our analysis. Foreseeability is primarily about there being sufficient clarity as to the circumstances in which and the conditions on which public authorities are empowered to resort to the discretionary power in question. That depends on the quality of the conditions and safeguards against abuse which apply to the exercise of a discretionary power to interfere with rights. In the context of surveillance powers, the ECtHR has emphasised that the law must ensure that "*measures are applied only when necessary in a democratic society" in particular by providing for adequate and effective safeguards and guarantees against abuse"*

[34] See *Big Brother Watch & ors v UK* (2022) 74 EHRR 17, [330] – [331].
[35] These terms mean the same thing.
[36] See e.g., *In re Gallagher* [2020] AC 185, [16] – [23].

(*Big Brother Watch & ors v UK* (2022) 74 EHRR 17, [334] ("***BBW***")).

52. In the context of "bulk" surveillance which, as we have explained, is analogous to the monitoring that would take place pursuant to 104 Notices, the ECtHR has set out minimum requirements as to what must be included in domestic law. These include: (1) the grounds upon which bulk interception might be authorised; (2) the circumstances in which an individual's communications might be intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties, and (6) the circumstances in which intercepted data may or must be erased or destroyed (*BBW* [348]).

53. The ECtHR has emphasised that there must be oversight at each stage of the process to assess the necessity and proportionality of the measures being taken. Crucially, it is well established that bulk surveillance "*should be subject to independent authorisation at the outset when the object and scope of the operation are being defined*" (*BBW*, [350] – [351]).[37] The CJEU has held that this requirement extends to the making of orders mandating CSPs to screen their users' communications data (which is in some senses similar to what is contemplated under Clause 104).[38] The ECtHR case law also establishes that there must also be supervision and independent *ex post facto* review of the exercise of bulk surveillance powers.[39] If these safeguards are absent, the measure in question will not be in accordance with the law.

54. In addition to these safeguards, the case law under Article 10 of the ECHR lays down additional requirements to protect journalistic sources and confidential journalistic material where the state may use investigatory measures to uncover this information. This can only be done if there is an "*overriding requirement in*

[37] The CJEU has reached the same view in relation to state access to communications data retained by communications service providers (*Tele Sverige*, [120]; *La Quadrature*, [139]).

[38] *La Quadrature* [179].

[39] *BBW*, [350]; *Tele Sverige*, [123].

the public interest" and there must be prior authorisation by an independent body. There are also other safeguards including a need for consideration of whether a less intrusive measure would satisfy that public interest requirement (*BBW* [444] – [445], [448]). The requirement for independent authorisation at this stage is in addition to the independent authorisation necessary prior to the interception taking place (in the case of bulk surveillance).

55. In the context of bulk surveillance, these enhanced safeguards do not apply when material is initially intercepted. They come into play where information has been collected and may be examined/analysed if this is done either intentionally to target a journalist/confidential journalistic material or there is *a high probability* that protected material will be uncovered (*BBW* [448]- [449]). Even if there is no such intention or probability prior to the examination of material, "*if and when it becomes apparent*" that material contains confidential journalistic information or information which may identify a source, its "*continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision making body invested with the power to determine whether continued storage and examination is justified by an overriding requirement in the public interest*" (*BBW* [450]). The ECtHR has not yet determined whether these safeguards apply equally to investigative NGOs and human rights defenders but there is a compelling argument that they do.[40]

56. In our view the clear analogies between Clause 104 (and CSS generally) and "bulk" interception (in respect of which the safeguards were developed) mean that the minimum safeguards required for "bulk" surveillance are highly relevant in determining what equivalent minimum safeguards would be necessary for surveillance under Clause 104 to be in accordance with the law.

57. Additionally, we consider that there is a strong argument that the enhanced safeguards designed to protect confidential journalistic sources and material apply to CSS in a similar way to their application in the context of bulk

[40] See the remarks of the Grand Chamber of the ECtHR concerning the role of NGOs in the *Magyar Helsinki Bizottsag* case (at [166]-[167]); see above.

interception. If monitoring were undertaken with the intention of identifying such material e.g., through the use of key words or selectors or there was a high probability of this happening, the additional safeguards would be triggered. Given the way that the relevant conduct is defined, this seems unlikely under 104 Notices. The enhanced safeguards for the protection of journalists and their sources are more likely to be relevant where CSS software flags communications as potentially containing CSEA or terrorism content, with human analysis necessary to verify whether they in fact fall into one of those categories. In that scenario, the safeguards would be triggered if it became apparent to a human analyst (or indeed artificial intelligence) that the communications may relate to confidential journalistic material / journalistic sources.

58. We accept that there are two important sources of legal safeguards that may protect the rights of those subject to 104 Notices:

    a) First, Clause 105 of the OLSB contains safeguards by circumscribing the exercise of the discretion to issue 104 Notices. But in our assessment, it does not contain all the safeguards necessary to ensure that interferences with ECHR rights are in accordance with the law.

    b) Second, we acknowledge that, for the purposes of this assessment, “law” is not confined to what is contained in statute. The guidance OFCOM will be required to issue will be relevant and may contain additional important safeguards to protect users’ rights. Therefore, at this stage we do not know the full legal framework within which 104 Notices may be issued, including OFCOM’s own guidance.

59. We nevertheless consider that there are serious deficiencies in at least four areas which mean that interferences arising from the monitoring of communications pursuant to Clause 104 would not be in accordance with the law/prescribed by law.

    a) The statutory scheme does not make provision for independent authorisation for 104 Notices even though it may require private bodies – at

the behest of a public authority – to carry out mass state surveillance of millions of user's communications. Nor is there any provision for *ex post facto* independent oversight. OFCOM, the state regulator, cannot in our opinion, be regarded as an independent body in this context.

b) The OLSB's definition of terrorism and CSEA content gives rise to a serious lack of clarity regarding the circumstances in which communications might be "identified" and taken down under Clause 104. Relevant content is defined with reference to a wide range of offences but most of these cannot be committed through communicating material alone. Similarly, the current lack of clarity as to what may constitute a private or public communication in the context of terrorist content, is inadequate and potentially arbitrary.

c) There is a marked absence of guidance on the procedure to be followed for examining communications which are "identified" by accredited technology or through other technology developed or sourced by CSPs pursuant to a 104 Notice. That is significant given that the conduct targeted by Clause 104 is defined in such a way that the examination of communications appears necessary to determine whether they satisfy the criteria for identification.

d) There are no enhanced safeguards to protect journalistic sources and/or confidential journalistic material. Critically, when a CSP examines communications to assess whether they contain terrorism or CSEA content, and it becomes apparent that those communications may relate to journalists/their sources, the proposed framework does not provide for the safeguards required by Article 10 of the ECHR to apply.

In relation to (a) and (c) above, in particular, it is not obvious how these deficiencies could be resolved through any guidance produced by OFCOM.

Necessary in a democratic society

60. In our opinion there are serious doubts about whether Clause 104 can be regarded as proportionate[41] and, therefore, necessary in a democratic society.

61. The starting point is, as we have said, this provision empowers the state to mandate, generalised, indiscriminate, bulk surveillance of the content of the communications of millions of people across a very wide range of platforms. For the reasons we have explained, the monitoring will necessarily involve human analysis of large numbers of communications to "identify", "take down" or "prevent individuals from encountering" content falling within two categories of content that Clause 104 targets. Notices issued under Clause 104 will therefore give rise to very significant interferences with the Article 8 and Article 10 rights of communications service users.

62. There can be no doubt about the importance of detecting and preventing the distribution of child sexual abuse material online. Nor can there be any doubt about the importance of preventing and detecting terrorist activity. But the validity of those objectives is not determinative of the proportionality of Clause 104. Moreover, for the reasons we have explained, surveillance mandated through Clause 104 would not be confined to these objectives. It would target content that may have nothing to do with proscribed imagery and which goes far beyond content whose communication constitutes a criminal offence. Content caught by Clause 104 may be no more than evidence of a wide range of criminal offences. It appears that terrorism content identified through CSS would not even need to be reported, beyond existing limited legal requirements contained in other legislation. The surveillance measures would not, therefore, necessarily contribute to law enforcement taking action against such offending.

63. Given the extensive intrusion with the rights of third parties, the weight attributable to the purpose of surveillance pursuant to Clause 104 is relevant to

[41] The ECtHR has not addressed the proportionality of bulk surveillance regimes and has instead subsumed this into the assessment of whether measures are in accordance with the law (e.g., *BBW* [334]). The CJEU has taken a similar approach because its case law in this area links proportionality to the existence of clear rules and safeguards against abuse (e.g., C-623/17 *privacy international v Foreign Secretary* [2021] 1 WLR 4421, [68] and [76]).

striking the balance between the competing rights and interests in play. These are matters that legislatures and courts have grappled with in other contexts.

a) It is notable that "bulk" interception and equipment interference under the IPA can only be used where necessary (i) in relation to overseas communications; (ii) in the interests of national security (alone) or (ii) in the interests of national security *and* for the purpose of preventing or detecting serious crime or the economic wellbeing of the UK in so far as that is relevant to national security.[42] Such powers cannot be used solely in respect of the prevention and detection of serious crime between UK users, let alone less serious crime. That legislative choice appears to have been made because lesser aims were not deemed to justify the serious interference with rights arising from bulk surveillance.

b) The CJEU's case law on legislative provisions concerning communications data is also instructive in this regard. The jurisprudence makes clear that mandating general, indiscriminate retention of this kind of information will be disproportionate (for the purposes of the rights to privacy and freedom of expression) unless the state is "*confronted with a serious threat to national security which is shown to be genuine and present or foreseeable*" (and other criteria are satisfied) (*La Quadrature*, [138] – [139], [168]). More targeted retention of such data is permissible for combating serious crime and preventing serious threats to public security but would be disproportionate if undertaken only for the purpose of combating crime falling short of serious crime (*La Quadrature*, [140]-[141], [168]).

c) In considering the proportionality of Clause 104, we think that the CJEU's judgement in *La Quadrature* is particularly instructive. A French law empowered the intelligence services to require communications service providers to implement automated data processing measures concerning traffic and location data for the purposes of identifying terrorist threats.[43]

[42] Section 138(1) and (2), and 178(1) and (2) of IPA 2016.
[43] *La Quadrature*, [41] – [44].

This discretionary power provided for the "*screening of all the traffic and location data retained by providers of electronic communications services carried out by applying the parameters set by national authorities*", which involved "*the undertaking on behalf of national authorities general and indiscriminate processing*".[44]

Unlike Clause 104, the French provision did not involve service providers screening the content of communications. The CJEU nevertheless held that this constituted a serious interference with privacy and freedom of expression rights, including because it is "*applied generally to all persons who use electronic communication systems including persons with respect to whom there is no evidence capable of suggesting their conduct might have a link to terrorist activities*".[45] Critically, the CJEU concluded the particularly serious interference occasioned by service providers screening traffic and location data (not content) would *not* be proportionate *unless* the state were facing a serious threat to national security which is shown to be genuine and present or foreseeable.[46]

64. Having regard to these principles, we consider there is considerable doubt whether the aims pursued are sufficient to justify the serious interference with privacy and freedom of expression of very large numbers of people.

65. Beyond the important differences as to the conduct/content that may justify the use of the powers, when compared to bulk powers under the IPA, there are two striking differences which go to the proportionality of Clause 104. The bulk powers discussed above, which we consider share similarities with surveillance under Clause 104, cannot be used in respect of communications that are wholly domestic. By contrast, Clause 104 permits bulk surveillance of wholly domestic communications and, indeed, it seems inevitable that most of the communications monitored would fall into that category.

---

[44] *La Quadrature*, [172].
[45] *La Quadrature*, [174].
[46] *La Quadrature,* [177].

66. Further, only the intelligence services (which have a relatively narrow mandate) are permitted to seek warrants to use these powers; they are not available to law enforcement. Surveillance under Clause 104, by contrast, could be mandated by a communications regulator. It is of significance, in our view, that when legislating to establish bulk powers, Parliament expressly limited the use of these powers in this way. That is indicative of concerns about the proportionality of permitting domestic bulk surveillance by a wider range of public bodies and/or for a wider range of purposes.[47]

67. Having made these observations, we acknowledge that the threshold for challenging in the abstract a legislative provision containing a discretionary power, such as Clause 104, as being "disproportionate" is high. It would need to "give rise to an unjustified interference" / "be bound to operate incompatibly" with Article 8 and or Article 10 in "all or almost all cases" or, at least, "a legally significant number of cases".[48] Notwithstanding that high threshold, for the reasons set out above, we Clause 104 may give rise to disproportionate interference with Article 8 and Article 10 of the ECHR in almost all cases. That is primarily because it provides for mass surveillance of the content of communications for purposes which are unlikely to justify such serious and widespread interferences with these rights.

68. Any legal challenge to the proportionality of interferences with Articles 8 and 10 arising from the implementation of CSS would be to an individual Notice. That would enable proportionality to be assessed with reference to the terms of a 104 Notice (including the specifics of the technology used) and evidence as to the operation of CSS. In our view, any such assessment would need to take into account any evidenced risk that mandating CSS could create security vulnerabilities in communications systems and/or devices, creating a further risk

[47] For discussion on limiting the use of bulk powers to overseas communications, see "A question of Trust" David Anderson QC June 2015, at §10.22 - 10.26 and Recommendation 44.

[48] *Christian Institute v Lord Advocate* 2016 SLT 805, [88] R*e Northern Ireland Human Rights Commission's Application for Judicial Review* [2018] HRLR 14, [76]; *Re McLaughlin* [2018] 1 WLR 4250, [43].

to the privacy rights of users. In other words, it is necessary to consider the collateral impact of any such measure on the rights of others.[49]

69. One of the reasons for the application of a high legal threshold when determining whether a statutory power is disproportionate and therefore incompatible with a fundamental right, is that the courts give deference to the assessment of the legislature in enacting that measure. The corollary of that constitutional deference is that during the passage of a bill through Parliament, there should be rigorous scrutiny of whether a proposed new measure is a proportionate interference with fundamental rights. Our observations on proportionality are therefore not limited to matters a court may consider on a subsequent challenge after the legislation has been enacted, but are also relevant to Parliamentarians in their scrutiny of the OLSB at this stage.

A waiver of privacy rights by consenting to use communications platforms

70. We have considered whether any aspect of this analysis would be altered by service providers making references to the risk of them being subject to 104 Notices and their use of CSS, in their terms and conditions to which their uses must agree (assuming the disclosure of this information were lawful). In our view, such notification and user agreement would not constitute a waiver of rights within the meaning of ECHR case law. In order to be valid, a waiver must be unequivocal, given in full knowledge of the facts, and based on informed consent (*Or u v Croatia* (2011) 52 EHRR 7, [178]). In respect of the latter the ECtHR has said that it must "*constitute a knowing and intelligent relinquishment of a right*" (*Bože v Latvia* (2017) application no. 40927/05, [69]).

71. In our assessment, consent would be very unlikely to qualify as being fully informed, and the right to privacy knowingly and intelligently relinquished, in circumstances in which a user of a service run by a private company must accept CSS in order to being able to communicate through the service. That issue would

[49] See by analogy, Kharitonov v Russia, [45]; see also the comments of the former Special Rapporteur on the freedom of expression (David Kaye) in respect of the weakening of encryption, in Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/29/32 (May 2015), para 35.

be accentuated in a digital environment in which most or all service providers were the subject of 104 Notices from OFCOM. Further, it seems implausible that users could or would be properly informed as to the risks involved, including in respect of weakening security on their devices and false positives (see above).

72. Support for this conclusion can be found in the approach to informed consent taken in in the UK GDPR, which legislation has its roots in and is underpinned by the right to privacy as enshrined in the ECHR and the Charter of Fundamental Rights of the EU. The UK GDPR defines consent as being "*freely given specific informed and unambiguous indication of the data subject's wishes by which he or she by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her*" (Article 4(11)). The European Data Protection Board has emphasised that *"[i]f consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given"*. If a service cannot be used without giving consent, any such consent is unlikely to be freely given.[50]

Common law rights

73. There is a long-established common law fundamental right not to have one's property seized or searched other than by authority of law which is reflected in the common law's aversion to general warrants.[51] A general warrant does not name individuals or premises and requires only "*the exercise of judgement or discretion by the official executing the warrant as to which individuals or which property should be targeted" (R (Privacy International) v IPT [2021] QB 936, [45]).* Clause 104 Notices may constitute a form of general warrant because the state would be mandating searches of digital communications on a generalised basis without targeting any particular person or device. The common law right not to be subject to such searches has been held to be engaged by thematic computer network exploitation (hacking) of devices.[52]

[50] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 (May 2020), p.7-8.

[51] *R (Privacy International) v IPT [2021] QB 936, [45] – [48]*

[52] Ibid.

74. Pursuant to the common law principle of legality, this right cannot be overridden unless this is done through express statutory wording, or by necessary implication.[53] The IPA is an example of where Parliament has done this. However, in our opinion Clause 104 does not (or would not in its current form) expressly override the common law right not to be subject to such searches on the basis of a general warrant. It does not specifically authorise the search of information (including the content of communications) on an individual's device. Nor does it do so by necessary implication. The consequence of this is that, if used in the way contemplated, this is likely to be in breach of users' fundamental rights at common law.

[53] *R v Secretary of State for the Home Department*, Ex p Simms [2000] 2 AC 115, p.1

MATTHEW RYDER KC
AIDAN WILLS
Matrix
31 October 2022