=RE: ONLINE SAFETY ACT:

THE DESIGNATION OF END-TO-END ENCRYPTION AS A RISK FACTOR

_____

LEGAL OPINION

_____

INTRODUCTION & SUMMARY OF OPINION

1. We are instructed by 89UP and the Index on Censorship to advise on whether OFCOM's characterisation of end-to-end encryption ("**E2EE**") as a "*risk factor*" which User-to-User ("**U2U**") services (we shall refer to the providers of U2U services as "**service providers**") must take account of in their risk assessments under the Online Safety Act 2023 ("the **OSA**") is compatible with the right to respect for private and family life and correspondence under Article 8 of the European Convention on Human Rights ("the **Convention**"). OFCOM designates E2EE as such in various November 2023 draft documents (and in particular its draft Risk Profiles) produced in fulfilment of its obligations as the regulator under the OSA (we use "**guidance**" as a shorthand to refer to these documents in the round). We are also asked to consider how this requirement interacts with service providers' duties concerning the rights to privacy and freedom of expression under s 22 of the OSA and their obligations under the UK GDPR. We understand that those instructing us wish to publish this opinion.

2. In summary, our advice is as follows:

A) OFCOM's identification of E2EE as a risk factor in its Risk Profiles (which must be taken into account by service providers when undertaking their own risk assessments) does not in itself amount to any direction or requirement to take any steps which would remove or weaken E2EE on the services in question.

B) If the duties in s 9, 10 of the OSA (taken with the OFCOM Risk Profiles) were interpreted and applied in a way and that led to service providers being compelled to weaken encryption on their messaging services in order to mitigate and manage risks identified in respect of E2EE, this may give rise to interferences

with users' rights under Articles 8 and 10 of the Convention, which may be imputable to the state.

c) In our opinion, however, these duties do *not* require service providers to take such steps. That is because, in short:

i. when implementing any measures to mitigate or manage risks service providers must, per s 22 of the OSA, have particular regard to service users' rights to freedom of expression and privacy (including data rights);

ii. service providers are only required to implement measures if they are "proportionate" which, it is strongly arguable, includes proportionality with reference to the privacy and freedom of expression rights of service users – the Article 8 case law set out in *Podchasov v Russia* indicates that measures which would have the effect of weakening encryption for all services users are unlikely to be proportionate for the purposes of Article 8 of the Convention; and

iii. service providers are under other legal obligations, including ensuring data security under the UK GDPR, which would be relevant when implementing any measures in response to risk assessments – the duties under the OSA do not displace those obligations.

d) We do not consider that OFCOM's identifying the functionality of E2EE communications as a risk factor is incompatible with Convention rights or otherwise unlawful. However, OFCOM's draft guidance does not contain sufficient recognition of the serious risks to the rights to respect for private life and correspondence and freedom of expression posed by service providers taking measures (in response to risk assessments or otherwise) which would undermine encryption. In the light of the European Court of Human Rights' ("**ECtHR**") decision in *Podchasov*, which postdates the draft guidance, this is something which, in our view, could helpfully be reflected in the applicable guidance.

STATUTORY AND POLICY FRAMEWORK

3. The starting point is the illegal content risk assessment duties imposed on U2U services by s 9 of the OSA. Among those duties is a requirement to "*carry out a suitable and sufficient illegal content risk assessment at a time set out in, or as provided by, Schedule 3"* (s 9(2)). The section explains that an *"illegal content risk assessment"* of a service of a particular kind is *"an assessment of [specified] matters, taking into account the risk profile that relates to services of that kind"* ("**the Risk Assessment Duty**"). This includes an assessment of the following factors of particular relevance to the issues with which this opinion is concerned:

> *(b) the level of risk of individuals who are users of the service encountering the following by means of the service—*
> *(i) each kind of priority illegal content (with each kind separately assessed), and*
> *(ii) other illegal content, taking into account (in particular) algorithms used by the service, and how easily, quickly and widely content may be disseminated by means of the service;*
>
> *(c) the level of risk of the service being used for the commission or facilitation of a priority offence;*
>
> *(d) the level of risk of harm to individuals presented by illegal content of different kinds or by the use of the service for the commission or facilitation of a priority offence;*
>
> *(e) the level of risk of functionalities of the service facilitating the presence or dissemination of illegal content or the use of the service for the commission or facilitation of a priority offence, identifying and assessing those functionalities that present higher levels of risk; […]*
>
> *(h) how the design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.* [emphases added]

4. The notion of "risk profiles" is important. Section 9(6) explains that this refers to the risk profiles for the time being published under s 98 of the OSA which relate to the risk of harm to individuals presented by illegal content. Section 98 imposes three broad duties on OFCOM.

a) First, it must "*carry out risk assessments to identify and assess*" particular risks of harm (see s 98(1)) presented by U2U and other Part 3 services. Those assessments must, among other matters: "*identify characteristics of different kinds of Part 3 services that are relevant to such risks of harm, and assess the impact of those kinds of characteristics on such risks*" (s 98(2)) ("the **Risks Assessments**"). The "characteristics" of these services are broadly defined to include "*functionalities, user base, business model, governance and other systems and processes*" (s 98(11)). OFCOM has conducted assessments and released them in draft form for consultation: they are contained in *Volume 2: The causes and impacts of online harm*.

b) Second, OFCOM must reflect the findings of the risk assessments in a "*register of risks of Part 3 services*" ("**Register of Risks**") which must be published (s 98(4)). OFCOM has published a draft Register of Risks. This is also contained in *Volume 2: The causes and impacts of online harm*, Ch 6A.

c) Third, after conducting the Risk Assessments, OFCOM must prepare and publish "*risk profiles for Part 3 services which relate to that risk of harm*" (s 98(5), (7)) ("**the Risk Profiles**"). OFCOM has published draft Risk Profiles. These are found in Appendix A in *Annex 5: Service Risk Assessment Guidance* (November 2023) ("**Annex 5**"); it is this document which, we understand, has generated particular concern on the part of those instructing us. As explained above, once final, service providers will be under an obligation to take them into account when carrying risk assessments pursuant to their s 9 OSA duties.

5. The next part of the picture is OFCOM's duty to produce and publish guidance "*to assist providers of regulated user-to-user services in complying with their duties to carry out illegal content risk assessments under section 9*" as soon as reasonably practicable after publishing the first Risk Profiles (s 99(1), (6)) ("**the Risk Assessment Guidance**"). OFCOM has published draft Risk Assessment Guidance, which appears in *Annex 5*, with further commentary in *Volume 3: How should services assess the risk of online harm?* (November 2023), Ch 9. There is no specific duty on service providers to follow or take this Guidance into account when conducting their own risk

assessments pursuant to the Risk Assessment Duty. OFCOM has stated "*the Risk Assessment Guidance does not represent a set of compulsory steps that services must take, but rather is intended to assist services in fulfilling their legal obligations*."[1]

6. While the Risk Assessment Duty is a duty of process on U2U services, s 10 of the OSA imposes a series of what are, in essence, duties of outcome on these services. These include:

> *(2) A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to—*
> *(a) prevent individuals from encountering priority illegal content by means of the service,*
> *(b) effectively mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence, as identified in the most recent illegal content risk assessment of the service, and*
> *(c) effectively mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service (see section 9(5)(g)).*

7. Pursuant to s 10(4), this duty requires service providers "*to take or use measures"* in the particular areas *"if it is proportionate to do so*"- these include: "*(b) design of functionalities, algorithms and other features,"* and "*(e) content moderation, including taking down content*." The section goes on non-exhaustively to identify factors of particular relevance when assessing what is proportionate, including for the purposes of ss 10(2) and (4):

> *(10) In determining what is proportionate for the purposes of this section, the following factors, in particular, are relevant—*
> *(a) all the findings of the most recent illegal content risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to individuals), and*
> *(b) the size and capacity of the provider of a service.*

8. Sections 10(2)(c) and (10) provides the link between the Risk Assessment Duty and the duties of outcome under s 10. This connection is important because it means that a service provider cannot simply ignore the risks identified through such an assessment: they have to take *proportionate measures* to mitigate and manage those risks. We return to this below.

[1] *Volume 3: How should services assess the risk of online harm?* (November 2023), ¶9.11.

9. OFCOM is under a statutory duty (pursuant to s 41(1)) to prepare and issue codes of practice for service providers "*describing measures recommended for the purpose of compliance with the duties*" in, inter alia, s 10. In November 2023 OFCOM published draft *Illegal Content Codes of Practice for user-to-user services* for consultation. These appear at Annex 7, with further commentary in *Volume 4: How to mitigate the risk of illegal harms – the illegal content Codes of Practice*. While the OSA states that the measures set out in the codes are recommendatory, s 49 (on the relationship between the duties and codes of practice) provides that:

> *(1) A provider of a Part 3 service is to be treated as complying with a relevant duty[2] if the provider takes or uses the measures described in a code of practice which are recommended for the purpose of compliance with the duty in question.*
>
> *(2) A provider of a user-to-user service—*
> *(a) is to be treated as complying with the duty set out in section 22(2) (freedom of expression) if the provider takes or uses such of the relevant recommended measures as incorporate safeguards to protect users' right to freedom of expression within the law;*
> *(b) is to be treated as complying with the duty set out in section 22(3) (privacy) if the provider takes or uses such of the relevant recommended measures as incorporate safeguards to protect the privacy of users.*

10. It is clear that subsection (1) gives service providers a very strong incentive to follow the codes, notwithstanding the fact they only make recommendations. The effect of subsection (2) would appear to be, if and in so far as the codes do make provision for safeguarding users' freedom of expression and privacy, adopting those safeguards will discharge the duties in s 22 to have particular regard to those rights. There are some such safeguards in the draft code but none are concerned with the issue of E2EE.[3]

11. Finally, the OSA places U2U services under three duties in relation to users' right to freedom of expression and right to privacy "*when deciding on, and implementing, safety measures and policies*" (which are defined as measures designed to secure compliance with inter alia s 10: s22(8)):

---

[2] For present purposes, the relevant duty is s 10 of the OSA (see s 49(9)).

[3] See Annex 7, A4.25(c) and (d), A4.26 -33, which are said at A4.34 to be safeguards for freedom of expression and privacy.

a) First, a duty to "*have particular regard to the importance of protecting users' right to freedom of expression within the law*" (s 22(2));

b) Second, a duty to "*have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a user-to-user service (including, but not limited to, any such provision or rule concerning the processing of personal data)"* (s 22(3)); and

c) Third, when deciding on safety measures and policies, a duty to "*to carry out an assessment of the impact that such measures or policies would have on— (i) users' right to freedom of expression within the law, and (ii) the privacy of users; and (b) to carry out an assessment of the impact of adopted safety measures and policies on the matters mentioned in paragraph (a)(i) and (ii)"* (s22(4)).

12. For present purposes, the "*have particular regard*" duties appear to apply primarily when a service provider is deciding what measures to take to comply with its s 10 duties. There is no obligation on service providers to have particular regard to these rights when discharging their Risk Assessment Duty under s 9 of the OSA.

13. OFCOM is not under any duty to produce guidance to assist U2U services in complying with the duties in s 22. However, as a public authority, OFCOM is required to act compatibly with Convention rights when exercising its functions (including promulgating guidance etc) under the OSA: s 6(1) of the Human Rights Act 1998.

Relevant OFCOM assessments and policies/guidance

14. Below, we summarise the relevant sub-statutory policies/guidance and assessments produced (in draft form at this stage) pursuant and/or relevant to the abovementioned duties in the OSA.

Risk Assessment and the Risk Register

15. OFCOM's risk assessment is concerned with "*risks of harm*," meaning *"harm to individuals presented by (a) content on U2U or search services that may amount to the offences listed in the Act, and (b) the use of U2U services for the commission and/or facilitation of these offences*." It identifies E2EE as being a "functionality" (which is one of the four groups of characteristics around which the assessment of risk factors is structured) that "stands out" as posing a "particular risk."[4] The concern is primarily about people being able to avoid detection and moderation when engaging in illegal acts using U2U services, and their being attracted to those services for precisely those reasons. These risks are said to arise across most, if not all, of the twelve categories of illegal harm identified in the Risk Assessment.

16. The introduction to the draft register of risks also recognises (albeit not in especially strong terms) the benefits of E2EE:

> *"some of the risk factors, which the evidence has demonstrated are linked to a particular kind of illegal harm, can also be beneficial to users. This can be in terms of the communication that they facilitate, or in some cases fulfilling other objectives, such as protecting user privacy.*
>
> *For instance, end-to-end encryption guarantees a user's privacy and security of messages, but makes it harder for services to moderate for illegal content…."* (¶6.11-12).

Risk Profiles

17. The Risk Profiles document is based on the Risk Assessment and Risk Register. It contains detailed step-by-step guidance on identifying risk factors.

18. Under "User Communication Factors" (that is: functionalities that allow users to communicate with one another) "encrypted messaging" is identified as a specific risk factor (5c, p.59). The document states:

> *"End-to-end encryption guarantees a user's privacy and security of their messages, while at the same time making it more difficult for services to moderate for illegal content being sent on their service. If your service allows encrypted messaging, we would expect you to consider how this functionality can be used by potential*

[4] In *Volume 2:The causes and impacts of online harm*: see for example ¶¶6.12; 6B.24, 44-47; 6C.24; 6F.27; 6H.28, 44; 6J.34, 36, 38; 6K.28, 41-42; 6L.34; 6M.59; 6N.26; 6O.16, 34, 37, 40, 76-78; 6P.61,65; 6Q.19; pp.3, 23, 31, 33, 44-47, 44, 53, 63, 91, 139, 148, 165-168, 179, 202, 218, 227, 245, 263.

perpetrators to avoid monitoring of communications while sharing illegal content.. or conducting illegal behaviour."[5]

Codes of Practice

19. The draft Illegal Content Codes of Practice for U2U services are said to relate to the "*design, operation and use*" of a U2U service.[6] This code does not say anything about E2EE. However, the "content moderation" chapter of the codes contains a number of recommended measures which, if implemented, could, in principle, have implications for E2EE (see chapter A4 in Annex 7). That could be the case if, for example, implementing one or more of these measures would necessarily involve taking steps which weakened encryption on a particular messaging service or could not be implemented without removing an E2EE functionality. Whether the implementation of any such measures would in fact do so raises technical rather than legal questions. We have not at this stage been instructed as to any potential concerns in this regard.

ARTICLES 8 AND 10 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS

20. Service users' right to respect for private and family life and correspondence (under Article 8 of the Convention) and right to freedom of expression (under Article 10 of the Convention) are of relevance where measures are taken in respect of messaging and other communications services.

21. These rights are only directly enforceable against public authorities (and not directly against service providers). However, if public authorities compel private actors, such as the providers of U2U services, to take steps which interfere with (and may violate) Convention rights, those interferences may be imputable to the relevant public authority/the state (see for example: *Ekimdzhiev v Bulgaria*, App. No.70078/12, 11 January 2022 concerning legislative measures compelling the collection, retention and disclosure of communications data retention by communications service providers, and the *Pochasvov* case discussed below).

The *Podchasov* case

[5] There are further references to encryption where messaging services are highlighted as a risk factor (1b, p55).
[6] Annex 7, A1.5.

22. The ECtHR has recognised in the Article 10 context the important role of anonymity in "*promoting the free flow of ideas and information in*" including by protecting people from reprisals for their exercise of freedom of expression (*Delfi AS v Estonia* [2015] EMLR 26, [147] and [149]). But until recently the ECtHR had not considered the issue of E2EE and how measures which undermine E2EE may impact on the Convention rights of service users.

23. The ECtHR considered this for the first time in the case of *Podchasov v Russia,* App No. 33696/19, in which case judgment was handed down in February 2024 (after the draft OFCOM documents referred to above were promulgated). The case concerned an order issued to Telegram requiring it to disclose to the security service "*technical information"* including encryption keys, which would *"facilitate 'the decryption of communications since 12 July 2017 in respect of Telegram users who were suspected of terrorism-related activities'"* relating to particular phone numbers.

24. That order was made against the backdrop of legal obligations requiring service providers to (a) retain communications data for a year and the content of all communications for six months; and (b) provide the security service with the information necessary to decrypt communications. Telegram refused to hand over the information requested to decrypt the communications, contending that it could only give effect to this by creating a backdoor in its messaging system that would weaken E2EE for all users of the service. Ultimately this led to enforcement action being taken against Telegram but that was not in issue on this application – Telegram brought its own application (App. No. 13232/18) in the ECtHR but it appears that this case was communicated but never adjudicated upon following Russia's leaving the Convention.

25. Mr Podchasov was a Telegram user who argued that the requirement for service providers to retain communications data and content was a breach of his Article 8 rights. He also contended that:

> "it was technically impossible to provide the authorities with encryption keys associated with specific users of the Telegram messenger application. In order to enable the decryption of end-to-end encrypted communications it would be necessary to weaken the encryption technology used by the Telegram messenger application. However, because these measures could not be limited to specific

individuals, they would affect everyone indiscriminately" (at [57]).

26. The ECtHR held that authorities' potential access to retained communications and the concomitant obligation to decrypt them if they are encrypted constituted an interference with Mr Podchasov's Article 8 rights (at [58]). In respect of what the Court described as the "*statutory requirement to decrypt communications*," it made the following important observations:

> "Encryption … appears to help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. This should be given due consideration when assessing measures which may weaken encryption" (at [76]).
>
> "The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations ... However, it takes note in this connection of the calls for alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution"" (at [78]).
>
> "in the present case the … statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued" (at [79]).

27. In the light of this reasoning of the ECtHR, it is difficult to see how any state-mandated measures to undermine encryption on a messaging service, in circumstances where that risks weakening E2EE for all users, could be regarded as necessary in a democratic society for the purposes of Article 8(2) of the Convention. Pursuant to s 2(1) of the Human Rights Act 1998, the UK courts would be required to take into account the ECtHR's decision in *Podchasov* if the issue came before them.

ASSESSMENT

28. It appears that the focus of the concern raised by those instructing us is the Risk Profiles because, in respect of service providers, they are supported by the strongest legal obligation among the various draft OFCOM documents in which E2EE is raised as a risk factor: a duty to take account of these risk factors.

29. OFCOM's identification of E2EE as a risk factor does not of itself amount to any direction or requirement to take any steps which would remove or weaken E2EE on the services in question. There is, however, an understandable concern that, with E2EE identified as a risk factor in the Risk Profiles, which must be taken into account when service providers undertake their own statutory risk assessments pursuant to the duty in s 9 of the OSA:

    a) carrying out a suitable and sufficient illegal content risk assessment would inevitably lead to their having to identify an E2EE functionality in their own services as posing some risk of facilitating the presence or dissemination of illegal content or the use of the service for the commission or facilitation of a priority offence (indeed the Risk Profile OFCOM makes it clear that it would expect them consider how this functionality can be used by potential perpetrators to avoid monitoring of communications while sharing illegal content.. or conducting illegal behaviour); and

    b) in turn, service operators would be required to take measures (including in respect of the design of functionalities) to effectively mitigate and manage a risk, which would inevitably be found to exist, in order to comply with their duties under s 10 of the OSA; and

    c) that may result on their being obliged to take measures which would weaken E2EE.

30. If the combination of the duties in s 9, 10 and the OFCOM Risk Profiles were interpreted and applied in this way and that led to service providers regarding themselves as being compelled to weaken encryption on their messaging services, this may give rise to interferences with users' Article 8 and Article 10 rights which may be imputable to the state. However, we do not think that it possible or necessary to address this issue in the abstract because, on analysis, the regulatory scheme does *not* compel outcomes of this kind. That is because there are important qualifications and limits to the relevant obligations on service providers:

a) First, in respect of the position of Risk Profiles when discharging the Risk Assessment Duty, the obligation is to *take them into account*. That means that, while the Risk Profiles cannot simply be ignored, they do not in and of themselves compel any particular outcome in terms of the content of service providers' risk assessments. To take into account does not mean to follow and the weight to be given to the Risk Profiles is, in the first instance, and subject to regulatory oversight, a matter for service providers.

b) Second, in formulating their risk assessments service providers will also have to have regard to their other legal obligations under statute and at common law. These would include, for example, their obligations under the law of data protection, the common law of privacy, and contractual and equitable obligations of confidence. We deal with these further below as they are of primary relevance with reference to any measures taken in response to / on the back of risk assessments.

c) Third, pursuant to s 22(2) and (3) service providers are under a parallel duty to have *particular regard* to users' right to freedom of expression and their privacy (including data protection principles) when implementing measures to comply with duties under (among other provisions) s 10 of the OSA. As part of this process, pursuant to s 22(4) of the OSA service providers are *required* to carry out an assessment of the impact that any measures which may be taken in response to/to mitigate risks identified in a risk assessment would have on those rights. Such an assessment ought to factor in the human rights case law rights including, in particular, the decision of the ECtHR in *Podchasov*.

d) Fourth, regardless of the risks identified by a service provider in its risk assessment, it is only under an obligation to take such measures to mitigate and manage such risks as are proportionate. Section 10(10) of the OSA contains non-exhaustive factors to be taken into account in assessing proportionality which are concerned with the nature and gravity of the risks identified and the size of the company involved. In our opinion there is a strong argument that the determination of whether a measure is proportionate (for the purposes of s 10)

would also have to bring into the balance the privacy and freedom of expression rights of service users as identified in the case law. That is because in a context in which Convention rights are obviously in play (as the OSA acknowledges through s 22), the measure of proportionality has to take into account the impact on the enjoyment of other Convention rights.

e) If the level of interference with service users' rights to privacy and/or freedom of expression is so great as to outweigh the countervailing benefits to be derived from a measure designed to mitigate identified harms, the application of the mitigation measure would not be proportionate and thus not required under s 10 of the OSA. As noted above, if a particular decryption measure undermined or weakened encryption for all users of a service, the decision in *Podchasov* suggests that is unlikely to be compatible with Article 8.

f) Fifth, as noted above, service providers have other legal obligations which may be relevant to any steps that they can take in response to risk assessments and in order to comply with s 10 of the OSA. Chief among these are the duties which service providers as data controllers of personal data must comply with. Of particular relevance are: (i) Article 5(1)(f) of the UK GPDR which requires data controllers to process personal data "*in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"* and (ii) the related obligation in Article 32(1) of the UK GDPR to "*implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*" presented by the processing of personal data, including unauthorised disclosure of or access to the data. The encryption of personal data is a measure that may be taken to comply with these requirements. The flip side of this is that measures which weaken encryption and increase the risk of unauthorised disclosure or access to personal data on / communicated through a U2U service could cause a service provider to be in breach of these provisions.

g) We do not understand s 10 to require service providers to take steps which would require them to, for example, breach statutory obligations under the UK GDPR, or indeed common law duties, in order to comply with their duties under s 10. Had that been intended by Parliament, it would have expressly said so.

31. We do not consider that from a legal perspective there is anything inherently problematic about OFCOM identifying the functionality of E2EE communications as a risk factor on the basis that this makes moderation and the detection of illegal acts more difficult. At present, however, OFCOM's draft guidance (writ large) does not, in our view, contain sufficient recognition of the serious risks to the rights to respect for private life and correspondence and freedom of expression posed by service providers taking measures (in response to risk assessments or otherwise) which would undermine encryption. The treatment of this subject is limited to passing references, e.g. in the Risk Profiles, which provide no assistance to service providers in factoring in and ensuring the protection of these rights when seeking to comply with the duties under ss 9-10 and 22 of the OSA, in particular.

32. Given that the decision in *Podchasov* postdates the publication of the assessments and draft guidance it is understandable that the ECtHR's reasoning is not reflected in these documents. We consider that it would be of assistance to service providers (and ultimately service users), and avoid potential confusion, for the ECtHR's decision to be reflected in more detailed consideration of the human rights implications of service providers taking any measures which may weaken encryption on their services.

PHILLIPPA KAUFMANN KC

AIDAN WILLS

Matrix

29 November 2024