Irish Council for Civil Liberties

1st Floor
34 Usher's Quay
Dublin 8
T: +353 1 912 1640
E: info@iccl.ie
w: www.iccl.ie

Date: 25 March 2022 Your ref: Application. No.: 13232/18 Our ref:

TO: **SECTION REGISTRAR OF THE EUROPEAN COURT**
MR MILAN BLASKO
European Court of Human Rights
Council of Europe
F-67075 Strasbourg Cedex
France

By facsimile: +33 (0)3 88 41 27 30 and by post

Dear Sir,

WRITTEN SUBMISSION IN *TELEGRAM MESSENGER LLP v. RUSSIA* (13232/18)

1. Pursuant to your correspondence dated 4 March 2022, kindly find attached hereto a written submission on behalf of the Irish Council for Civil Liberties and 8 other organisations.

2. In terms of the Rules of Court, three copies of the written submission will also be submitted via registered post.

3. Kindly advise if anything further is required.

Yours faithfully,

_____

IRISH COUNCIL FOR CIVIL LIBERTIES (ICCL)
Liam Herrick (Executive Director)
Unit 11, First Floor, 34, Usher's Quay, Dublin 8
Email: liam.herrick@iccl.ie
Date: 25 March 2022

IN THE EUROPEAN COURT OF HUMAN RIGHTS

THIRD SECTION

Application no. **13232/18**
TELEGRAM MESSENGER LLP and TELEGRAM MESSENGER INC.
against Russia

Third party intervention submitted jointly by the Irish Council for Civil Liberties, the Canadian Civil Liberties Association; the Centro de Estudios Legales y Sociales; Centro de Estudios de Derecho, Justicia y Sociedad; Hungarian Civil Liberties Union; Kenya Human Rights Commission; KontraS; Legal Resources Centre; and Liberty ("**the Intervenors**")

lodged on **25 March 2022**

WRITTEN SUBMISSION

---

1. This submission is made pursuant to leave to intervene being granted, in terms of Rule 44 § 3, by the Vice-President of the Third Section of the European Court of Human Rights on 4 March 2022.

2. The Intervenors are independent human rights organisations which work to protect and promote fundamental rights, including the rights to freedom of expression and privacy. The Intervenors are all members of the International Network of Civil Liberties Organizations ("INCLO").

3. This submission addresses the three salient points of intervention detailed in the application to intervene dated 21 January 2021, namely that (a) emerging international standards on encryption emphasise the role that encryption plays in protecting freedom of expression and privacy; (b) "backdoors" to encrypted communications are irreconcilable with the principles of necessity and proportionality; and (c) there is a lack of data available to understand the scale and need for decryption based on the grounds of national security.

4. This submission does not address the facts or merits of the application.

A. Emerging international standards on encryption

5. Encryption, which may be applied to data in transit (e-mail, messaging, Internet telephony) and / or at rest (hard drives, cloud services),[1] aims to safeguard data from unwanted access and / or manipulation.

6. Encryption is a tool that supports a secure Internet, and facilitates secure financial transactions and private communications globally. When considering state requests for "backdoors" into secure communications, the primary issue is *not* the tension between individual or collective freedoms, privacy, and expressive rights and state security, but rather a consideration of the collective security of every user of a platform in proportionate balance with state interests in national security.[2] This is reinforced by the 2019 statement by the former US Attorney General, conceding that backdoors decrease security.[3]

7. Workarounds or loopholes to encryption can include finding, guessing, or compelling the encryption key; exploiting a flaw; accessing plaintext when in use; or locating a plaintext copy. Experts take the view that governments demanding the ability to obtain plaintext interferes with strong encryption and makes the Internet less secure.[4]

8. Today, with the increasingly global use of smartphones,[5] end-to-end encryption ("E2EE") is considered "the most basic building block" for digital

---

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye to the Human Rights Council, May 2015. A/HRC/29/32.

[2] Abelson, H., et al. (2015). Keys Under Doormats. Communications of the ACM. 58. 24-26: https://www.researchgate.net/publication/282525791_Keys_Under_Doormats.

[3] US Department of Justice: Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security, 23 July, 2019: https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

[4] Abelson, H., et al. (2015). Keys Under Doormats. Communications of the ACM. 58. 24-26: https://www.researchgate.net/publication/282525791_Keys_Under_Doormats.

[5] Almost every developed country had at least 90 per cent mobile phone penetration in 2017: *Global mobile consumer trends, 2nd edition Mobile continues its global reach into all aspects of consumers' lives*. Deloitte, 2017: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-global-mobile-consumer-survey-second-edition.pdf.

security on messaging apps, and many apps offer it by default.[6] Encrypting smartphones and devices helps protect against hacking and crime,[7] and promotes the right to impart information safely and securely online.

9. The privacy afforded by encryption provides advantages to populations who are discriminated against or face "reprisals or unwanted attention" by providing them with safe forums to congregate, organise, mobilise, build communities.[8] This includes, among others, investigative journalists, lawyers, human rights defenders, activists, and civil society organisations. It also allows people to seek, receive, and impart information — and promote "the free flow of ideas and information in an important manner" — without the risk of repercussions, disclosure, surveillance, or other improper conduct.[9] (See *Delfi AS v Estonia* (2015) application no. 64569 (GC) at [147] and [149].)

Encryption, anonymity, and the United Nations ("UN")

10. In 2011, the then UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue ("La Rue"), cautioned against states reducing people's ability to shield themselves from arbitrary surveillance, by limiting encryption.[10]

11. In 2015, La Rue's successor, David Kaye ("Kaye"), highlighted that in censorious environments,[11] individuals, and especially lawyers, journalists, human

---

[6] Portnoy, E. *Building a Secure Messenger*, Electronic Frontier Foundation, 29 March 2018: https://www.eff.org/deeplinks/2018/03/building-secure-messenger.

[7] Center for Democracy and Technology, *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, 3 March 2016: https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government-surveillance/ .

[8] Noman, Helmi, Arab Religious Skeptics Online: Anonymity, Autonomy, and Discourse in a Hostile Environment (February 4, 2015). Berkman Center Research Publication No. 2015-2, https://ssrn.com/abstract=2560491 or http://dx.doi.org/10.2139/ssrn.2560491. Also the Egyptian LGBTQ community increasingly relies on encrypted communications such as Signal, https://www.alaraby.co.uk/english/indepth/2017/11/27/egypts-morality-police-get-on-grindr.

[9] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the Human Rights Council, May, 2015, A/HRC/29/32 par. 6.

[10] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Addendum, Communications to and from Governments, 16 May 2011, A/HRC/17/27, pars. 54-55.

[11] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the UN Human Rights Council, May 2015. A/HRC/29/32, par. 12.

rights defenders, and activists, may be forced to rely on encryption to circumvent restrictions,[12] and to transmit information beyond their borders.[13] Kaye advised that states should not restrict encryption; blanket prohibitions fail to be necessary and proportionate; states should avoid backdoors, weak encryption standards, and key escrows;[14] and he called for encryption by design and default.[15]

12. Additionally, Kaye advised that court-ordered decryption should only be permitted on a case-by-case basis applied to individuals pursuant to "transparent and publicly accessible" legal criteria which meet the requirements of Article 19(3) of the ICCPR and are subject to prior judicial authorisation and due process safeguards.[16]

13. In a subsequent 2016 report, Kaye warned, in response to measures such as E2EE, that states were seeking to compel firms to create loopholes in their products on their behalf.[17] That year, the European Union Agency for Cybersecurity ("ENISA") and Europol advised that "intentionally weaken[ing] technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well."[18]

14. In 2017, Kaye found that unnecessary and disproportionate measures to undermine encryption had increased globally, threatening people's freedom of expression and security. He cautioned that states had not provided sufficient evidence that such vulnerabilities were the least intrusive means of protecting national security, given the other tools at their disposal.[19] That year, a UN Human

---

[12] Ibid.
[13] Ibid, par. 25.
[14] Ibid, par. 60. Also for a discussion of key escrows and their vulnerabilities see Abelson et al., The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption (1997). https://doi.org/10.7916/D8GM8F2W.
[15] Ibid, par. 63.
[16] Ibid, par. 60.
[17] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the UN Human Rights Council, May 2016. A/HRC/32/38, par. 62.
[18] Joint statement by ENISA and Europol, "On lawful criminal investigation that respects 21st century data protection", 20 May 2016.
[19] Reference to traditional policing and intelligence, and transnational cooperation, also wiretapping, geo-location and tracking, data-mining, and traditional physical surveillance. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the Human Rights Council, March 2017. A/HRC/35/22, par. 21.

Rights Council resolution called on states to stop interfering with encryption unless they complied with international human rights law.[20]

15. In 2018, Kaye reported that the challenges faced by users had "increased substantially"[21] since 2015, highlighting how Pakistan had passed laws cracking down on the use of encryption; Iran banned encryption; Turkey arrested thousands of citizens for the alleged use of an encrypted messaging app;[22] and there had been "mounting" state pressure on companies to install encryption "backdoors".[23]

16. As a result, Kaye recommended, among others, that states adopt laws that protect the use of encryption tools; that laws should be established to specify clearly that restrictions on encryption tools are permitted only in *exceptional* circumstances; i.e. when they satisfy the requirements of legality, necessity, proportionality, and legitimacy of objective; that states should not require private actors to facilitate backdoor access; and that laws providing for court-ordered decryption or hacking should require the authorisation, on a case-by-case basis, of an independent and impartial judicial body of the proposed decryption or hacking order, and that the judicial body should review the order to ensure it meets the requirements of legality, necessity, proportionality, and legitimacy of objective.[24]

17. In 2020, the United Nations ("UN") General Assembly adopted a draft resolution, "The right to privacy in the digital age", calling on states not to interfere with encryption, emphasising that encryption and anonymity are important to ensure the enjoyment of the rights to privacy and expression.[25] The UN Office of the High Commissioner for Human Rights has also detailed, at length, the value of the Internet to expression, privacy, and anonymity, and the capabilities of states, corporations, and criminals, to interfere with these rights.[26]

---

[20] Human Rights Council, U.N. Doc. April 2017. A/HRC/RES/34/7 par. 9.

[21] Research Paper 1/2018, June 2018, Encryption and Anonymity follow-up report, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, par 2: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

[22] Ibid, par 11. See, also, *Alparslan Altan v Turkey* (2019) application no. 12778/17.

[23] Ibid, par 13.

[24] Ibid, pars 47-51.

[25] The right to privacy in the digital age: resolution adopted by UN General Assembly (75th session 2020-2021) A/RES/75/176, par.9.

[26] See Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30 June 2014 (A/HRC/27/37); UN General Assembly Resolution 68/167, 18 December 2013

In doing so, the UN has repeatedly voiced concern over attempts to weaken encryption due to these interferences.[27]

18. In 2021, Kaye's successor, Irene Khan, reiterated her predecessors' calls and advised that anonymity and encryption are "an essential facet of women's enjoyment" of freedom of expression online.[28]

B. Backdoors to encrypted communications are neither necessary nor proportionate

19. In 2015, Kaye reported that regulation of encryption often fails to meet freedom of expression standards because: (i) restrictions have generally not been shown to be necessary to meet a particular legitimate interest; and (ii) they disproportionately impact expressive rights.[29] Referring to anonymity and encryption as the "leading vehicles for online security",[30] Kaye reported that the "universal position among technologists" is that:

> "[t]here is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind … intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online."[31] (Own emphasis.)

20. In relation to backdoors, even if for legitimate purposes, Kaye reported that they threaten the privacy necessary for exercising freedom of expression,[32] advising that "[i]ntentional flaws invariably undermine the security of all users online" and "[g]iven its widespread and indiscriminate impact, back-door access would affect, disproportionately, all online users."[33]

(available at A/RES/68/167); Report of the Special Rapporteur, 10 August 2011 (A/66/290); and Report of the Special Rapporteur, 17 April 2013 (A/HRC/23/40).

[27] For a more detailed discussion about how backdoors undermine the security of all online users see PACE, Committee on Legal Affairs and Human Rights, Report on Mass Surveillance (2015); and Schneier, B., Data and Goliath, W. W. Norton & Company, (2015) 147–48.

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan to the UN General Assembly, July 2021. A/76/258, par. 90.

[29] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the Human Rights Council, 2015. A/HRC/29/32, par. 39.

[30] Ibid, par. 1.

[31] Ibid, par. 8.

[32] Ibid, par. 43.

[33] Ibid, par. 42.

Article 10 of the European Convention on Human Rights

21. The Grand Chamber recently found that an entity which provides a platform for others to exchange information may be regarded as exercising Article 10 rights, as "providing a forum or third-party content and imparting information and ideas itself . . . are inseparably intertwined." (See *Magyar Kétfarkú Kutya Párt v Hungary* (2020) application no. 201/17 (GC) at [91] and *Tamiz v United Kingdom* (2017) application no. 3877/14 at [90].)

22. Relying on *Magyar Kétfarkú Kutya Párt* and *Tamiz*, this precedent may be extended to communications service providers who are compelled by statutory requirements to, for example, hold and make available encryption keys or create backdoors which enjoin not only the expressive rights of users of the platform but the rights of the communications service provider itself.

23. To the extent that Article 10 rights of a communications service provider are engaged, an order compelling the decryption of a particular device or specific communications may make not only the target users but all users more vulnerable. This may be analogous to authorising targeted surveillance and / or interception. Equally, any law compelling communications service providers to make *all* encryption keys available may be analogous to authorising bulk or mass surveillance and / or interception.

24. In this event, this Court has provided a set of criteria and safeguards in relation to both targeted and bulk or mass surveillance, which must be set out in law in order to avoid disproportionate interference and "abuses of power". (See *Zakharov* at [231]; *Big Brother Watch & ors v United Kingdom*, application nos. 58170/13, 62322/14, and 24960/15 (GC) at [335], [336], and [348] – [350].)

25. Additionally, in the context of secret surveillance, the Grand Chamber has, to an extent, elided to the requirements of "prescribed by law" in the Article 10(2) analysis, providing that:

> "[d]omestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[34]

[34] *Roman Zakharov v Russia* (2015) application no. 47143/06 (GC) at [229] ("*Zakharov*").

26. The requirement that an interference with Article 10 must be "necessary in a democratic society" comprises three sub-elements: (a) it must correspond to a "pressing social need"; (b) the measure must be *proportionate* to the legitimate aim; and (c) the reasons given to justify the interference must be "relevant and sufficient".

27. In terms of proportionality, the Court has held that States enjoy a wide margin of appreciation when it comes to the selection of measures to achieve the aim of protecting national security. (See *Zakharov* at [229].) However, the Court has also held that challenges, even those posed by terrorism, do not absolve states from their Article 10 obligations. (See *Döner and Others v Turkey* (2017) application no. 29994/02.)

28. In this regard, weakening encryption for one, weakens it for all, and the collateral impact of a measure on persons not party to an application is relevant to the necessity and proportionality assessment, particularly if there are less intrusive measures available such as judicially authorised decryption of a seized device and judicial orders to compel a user to provide a password and/or code. (See *Voskuil v Netherlands* (2008) application no. 64752/01 at [65] and [71].)

29. While Article 10 is not an absolute right, the Court has found that "the exercise of powers to interfere with the right to impart information must be clearly circumscribed to minimise the impact of such measures on the accessibility of the internet",[35] and that domestic procedures, for the judicial review of such measures, must consider the rights of Internet users generally and any collateral effects.[36]

C. Insufficient data to identify the need for decryption mechanisms

30. Evidence of law enforcement agencies across member states dismantling organised crime groups who used encrypted communications exists.[37] However,

---

[35] *Vladimir Kharitonov v Russia* (2020) application no. 10795/14 at [43].
[36] Ibid, par.45.
[37] See Europol Press Release. Operational Task Force Leads to Dismantling of One of Europe's Most Prolific Crime Groups Behind €680 Million Operation, May 22, 2019. Osborne, Charlie. Phantom Secure CEO pleads guilty to providing drug cartels with encrypted phones, ZDNet, October 4, 2018. M. van Dinther, Politie breekt met success in op versleuteld netwerk van criminelen en noemt hete en doorbraak bij de opsporing, de Volkskrant, November 06, 2019.

empirical data outlining the number of investigations and prosecutions that have been thwarted by encryption, and the rate of change of the same, is lacking.[38] In a 2019 report on encryption and criminal investigations in Europe, Europol and Eurojust reported that official statistics on how much digital evidence is seized in criminal investigations, or on the number of investigations that require decryption of data, are not available.[39]

31. Follow-up reports in 2020[40] and 2021[41] failed to provide such statistics with those reports simply noting encrypted communication was a "recurring" issue.[42] Academics have also highlighted the lack of evidence to show the true extent of the problem.[43] This lack of empirical data — particularly in a "golden age for surveillance"[44] — detracts from necessity arguments and consequently leaves proportionality analyses largely unsubstantiated, which chimes with Kaye's view that states often fail to provide public justification for restrictions or the need to breach encryption via backdoors.[45]

D. Conclusion

32. To the Intervenors' knowledge, this is the first time the issue of the encryption (and decryption) of communications has come before the Court. As a result, this case raises issues of profound importance in relation to freedom of expression and privacy.

Encrypted Devices Found as Gardaí carry out organised crime raids, The Irish Times, September 19, 2018.

[38] Lewis, James; Zheng, Denise; Carter, William A. The Effect of Encryption on Lawful Access to Communications and Data. Center for Strategic and International Studies, p. 30, February 2017.

[39] Europol and Eurojust. First report of the observatory function on encryption, January 2019.

[40] Europol and Eurojust. Second report of the observatory function on encryption, February 2020.

[41] Europol and Eurojust. Third report of the observatory function on encryption, July 2021.

[42] Ibid. See page 8 in the 2020 report and page 18 in the 2021 report.

[43] Walden, Ian. (2018). 'The Sky is Falling!' – Responses to the 'Going Dark' problem. Computer Law & Security Review. 34.

[44] Swire, Peter. The Golden Age of Surveillance, July 2015; and Granick, Jennifer Stisa. If the Government Had Its Way, Everything Could be Wiretapped, ACLU, February 2019.

[45] Research Paper 1/2018, June 2018, Encryption and Anonymity follow-up report, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.

33. The Intervenors take the view that contrary to the viewpoint that encrypted spaces are dark "zones of unlawfulness"[46] which law enforcement agencies must pierce and access, encryption enables the full enjoyment of fundamental rights, including the rights to freedom of expression and privacy.

34. Expert technologists have repeatedly cautioned that claims[47] that exceptional access "backdoors" can be used without compromising the security of encrypted systems as a whole is a fallacy.[48] Such "backdoors" give rise to a situation where that "protected" insecurity is only as strong as the rules and technical protections that safeguard it. To trust in such a system assumes that all laws at all locations are sufficient, and that malicious and nefarious actors are incapable of targeting that insecurity. This is clearly not the case.[49]

35. It bears reaffirming that when considering state requests for "backdoors" into secure communications, the primary consideration *is* the collective security of every user of a platform in proportionate balance with state interests in national security.[50] It *is not* the tension between individual or collective freedoms, privacy, and expressive rights and state security.

DUBLIN, IRELAND

25 MARCH 2022

---

[46] See above n 3.

[47] Levy, I. and Robinson, C. Principles for a more informed exceptional access debate (Lawfare), November 29, 2018: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

[48] Schneier, B. Evaluating the GCHQ exceptional access proposal (Lawfare), January 17, 2019: https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal.

[49] Callas, J., When you have data, they will come, ACLU, July 23, 2019: https://www.aclu.org/blog/privacy-technology/when-you-have-data-they-will-come?redirect=blog/when-you-have-data-they-will-come.

[50] Landau, S., Surveillance or Security? The Risks Posed by New Wiretapping Technologies, MIT Press, 2011; Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary House of Representatives, 112th Cong. 23–34 (2011) (statement of Prof. Susan Landau): https://www.govinfo.gov/content/pkg/CHRG-112hhrg64581/pdf/CHRG-112hhrg64581.pdf.