FAX COVER SHEET

TO	Section Registrar
COMPANY	European Court of Human Rights
FAX NUMBER	33388412730
FROM	Clara Lilley
DATE	2021-12-06 13:56:43 GMT
RE	Privacy International's Intervention in Podchasov v. Russia (App. No. 33696/19)

COVER MESSAGE

DearSir/Madam,

Please find attached Privacy International's written submissions in the case of Podchasov v. Russia (App. No. 33696/19).

Please do not hesitate to contact us should you require further information.

We would be grateful if you could confirm safe receipt.

Yours faithfully,

Ioannis Kouvakas
Legal Officer and Acting General Counsel
Privacy International

European Court of Human Rights
***Anton Valeryevich PODCHASOV v. Russia, Application no. 33696/19* WRITTEN**

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL

I. Introduction and Summary of intervention

1. This intervention is submitted by Privacy International (PI, the "Intervener"), pursuant to leave granted by the President of the Section in accordance with Rule 44(3) of the Rules of the Court. PI is a non-profit, non-governmental organisation (Charity Number: 1147471) that research and advocates globally against government and corporate abuses of data and technology.

2. *Podchasov v. Russia* concerns the Russian law obliging telecommunications service providers to indiscriminately retain content and communications data for certain time periods, as well as a 2017 disclosure order by the Russian Federal Security Service requiring Telegram Messenger company to disclose technical information which would facilitate "*the decoding of communications*". As such, it presents the Court with an exceptionally unique opportunity to assess the seriousness of interferences that seek to weaken modern encryption tools and to uphold the rights of millions of users, by applying the Convention in the digital era.

3. This submission aims to assist the Court in its assessment of the compatibility of the Russian legislation and disclosure order with Article 8 of the Convention. It is structured in four parts: First, it describes how encryption, including end-to-end encryption works, and why it has come to play a vital role for everyone around the globe as an enabler of the protection of privacy, as well as other human rights. Second, it discusses the implications of various measures that seek to facilitate the decoding of encrypted communications, which, in line with the Court's case-law on communications surveillance, should be viewed as a serious interference with the right to respect for private life and correspondence. Third, it argues that imposing obligations upon telecommunications service providers to actively alter the software they are offering to users, by inserting back-doors or essentially degrading its security, violates states' positive obligations to protect the right to respect for private life and correspondence. Fourth, it submits that measures requiring the decoding of encrypted communications cannot be limited to what is necessary in a democratic society, due to their indiscriminate character and the fact that they inevitably compromise the integrity and security of communications for billions of users globally.

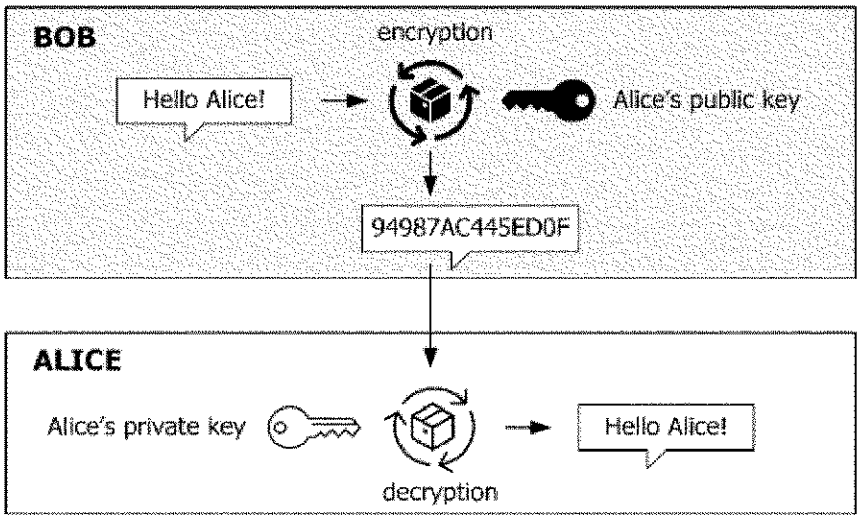
II. How encryption works and why it is important for modern communications

4. Information security is an enabler of privacy, and in turn, keeps individuals safe.[1] As more of people's lives are lived in the digital realm, communication security tools, such as encryption,

[1] More recently, the United Nations Human Rights Council emphasised the importance of encryption for ensuring "the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association" in its Resolution on the Right to Privacy in the Digital Age, A/HRC/48/L.9/Rev.1, 7

are increasingly important to the protection of human rights, including the right to privacy. Communication security tools give individuals access to safe and private spaces for personal development where they can communicate without unwarranted interference.[2]

5. Encryption is a way of securing communications using mathematical algorithms that protect content data while in transmission or storage.[3] The method relies on the generation of mathematically related numbers, unique for each recipient. Those two numbers, called 'keys', are used to cipher and decipher a message. For each communication, one of the two keys, the 'public' one is distributed to anyone that can send a message to the recipient, while the corresponding 'private' key is exclusively used by the recipient. The 'private' key must be kept secure, and not shared with anyone. Advanced applications used for communications in modern devices, such as mobile phones, generate this pair of keys for their user. By relying on the "*public-key cryptography*" technique, anyone can send an encrypted message that only the recipient can unscramble.[4]



6. Encryption, hence, relies on the process of merging a message ('plaintext' – the content of the message) with a passphrase or other data such as a file (commonly referred to as an 'encryption key') to produce a 'ciphertext' that is indecipherable to users who do not have the encryption key. In order to make the message coherent, an individual must use a correct key to decrypt the ciphertext and convert it back to readable plaintext. In other words, the sender of the message uses their encryption key to turn a readable message into scrambled, unreadable text. In return, the message's recipient uses an encryption key to make the message readable. If the message is intercepted in transit, it will be unreadable.

---

[2] PI, Securing Safe Spaces Online: Encryption, online anonymity, and human rights, https://privacyinternational.org/sites/default/files/2018-02/Securing%20Safe%20Spaces%20Online_0.pdf.

[3] Danielle Kehl, "Encryption 101", (Slate, 24 February 2015), http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html.

[4] PI, Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages.

7. One of the most robust forms of encryption is end-to-end encryption. With end-to-end encryption, a user encrypts the contents of a message on their own device and the messaging service or application sends an encrypted version of that message to a final recipient who then decrypts the message on their own device.[5] As the encryption and decryption of messages sent and received occurs on users' devices, full end-to-end encryption provides only the intended recipients – not even the communications service provider – with access to the content of the message, making it secure.[6]

8. Additionally, several messaging service providers, including Telegram, WhatsApp and Signal, have implemented 'forward secrecy',[7] which requires that the private keys for a connection are kept in an ephemeral storage. This basically means that every time a certain number of messages is sent, or a certain time period has lapsed, a new key is generated.[8] Accordingly, the key used to encrypt a previous message cannot be reconstructed once this has been transmitted or received. This provides users of end-to-end encryption messaging services with an additional layer of security, because, if a single key is compromised, the adversary will only have access to a limited number of messages. In fact, not even the communications services provider will be able to retroactively decrypt past messages. In the case of Telegram, a new key will be created once "*a key has been used to decrypt and encrypt more than 100 messages, or has been in use for more than one week, provided the key has been used to encrypt at least one message. Old keys are then securely discarded and cannot be reconstructed, even with access to the new keys currently in use*".[9]

9. It should be noted that end-to-end encryption protects only the content of electronic messages; the intermediaries would still be able to see the metadata accompanying the messages, such as subject lines, dates, sender, and recipient.[10]

10. Several actors have underscored the importance of encryption for safeguarding individuals' privacy, as well as for the effective exercise of other rights, including the right to freedom of expression.[11] In the words of UN High Commissioner for Human Rights "*it is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a Government's ability to break into its citizens' phones may lead to the*

---

[5] Nicole Perlroth, What Is End-to-End Encryption? Another Bull's-Eye on Big Tech, (New York Times, 19 November 2019), https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html.

[6] See, for example, Signal Support, 'How do I know my communication is private?', https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private-; WhatsApp, 'About end-to-end encryption', https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption.

[7] Telegram, for example, started supporting perfect forward secrecy as early as December 2014, https://telegram.org/blog/telegram-me-change-number-and-pfs#perfect-forward-secrecy.

[8] WhatsApp, WhatsApp Encryption Overview: Technical white paper (Version 3, October 2020), page 3, https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=ciRO7Acldu8AX_Mi-3r&_nc_ht=scontent.whatsapp.net&oh=6fc894bb719bdaf871c1c7f5464a9554&oe=61AE7799.

[9] Telegram, 'Perfect Forward Secrecy', https://core.telegram.org/api/end-to-end/pfs.

[10] Surveillance Self-Defense, A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? (29 November 2018), https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work.

[11] UN Office of the High Commissioner for Human Rights, Apple-FBI case could have serious global ramifications for human rights: Zeid (4 March 2016), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138.

persecution of individuals who are simply exercising their fundamental human rights".[12] In the June 2015 report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated that:

> Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment.[13]

III. Measures that seek to weaken encryption constitute a serious interference with Article 8 of the Convention

11. Despite the substantial weight encryption tools have nowadays attained as enablers of fundamental freedoms in the digital era, recent years have witnessed a plethora of efforts by governments across the world to introduce measures that seek to undermine these protections.[14] In 2013, the New York Times released documents demonstrating the United States National Security Agency's (NSA) efforts to weaken encryption, by deploying a variety of methods.[15] In 2016, Russia enacted anti-terrorism legislation requiring communications service providers to indiscriminately retain communications content and data and to be able to provide store, and to submit that data to law-enforcement authorities or security services in cases specified by law together with information necessary to decode electronic messages if they are coded.[16] In November 2018, UK politician Ian Levy and Crispin Robinson of the UK General Communications Headquarters (GCHQ) published a proposal for "*silently adding a law enforcement participant to a group chat or call*" ('ghost proposal').[17] Similarly, a draft discussion paper that was leaked in the summer of 2021 revealed details behind the European Commission's thinking about "*technical solutions to detect child sexual abuse in end-to-end encrypted communications*".[18]

---

[12] See UN Human Rights Council, Resolution on the Right to Privacy in the Digital Age, A/HRC/48/L.9/Rev.1, 7 October 2021.

[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32, 22 May 2015), para 12.

[14] Ibid, paras 38-46. See also PI, Securing Safe Spaces Online: Encryption, online anonymity, and human rights, https://privacyinternational.org/sites/default/files/2018-02/Securing%20Safe%20Spaces%20Online_0.pdf.

[15] The New York Times, Secret Documents Reveal N.S.A. Campaign Against Encryption, https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

[16] See Federal Law Number 375-ФЗ of 6 July 2016 on Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure natural harmlessness (Федеральный закон от 6 июля 2016 г. № 375-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения natural harmlessness").

[17] Ian Levy/Crispin Robinson, Principles for a More Informed Exceptional Access Debate (Lawfare, 29 November 2018), https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

[18] 'Technical solutions to detect child sexual abuse in end-to-end encrypted communications', https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf.

12. Both the provisions contained in the Russian counter-terrorism legislation and the aforementioned 'ghost proposal' by the GCHQ would essentially oblige communications service providers to build workaround that enables a third party to see the plain text of an encrypted conversation without notifying the participants.[19] In order to achieve this result, communications services providers, like Telegram, would have to actively implement two fundamental changes in the way their end-to-end encryption systems operate: first, service providers would have to surreptitiously inject a new public key into a conversation in response to a government demand. This would turn a two-way conversation into a group chat where the government is the additional participant or add a secret government participant to an existing group chat. Second, to ensure the government is added to the conversation in secret, service providers would have to change their software so that it would alter the encryption schemes used and/or mislead users by suppressing the notifications that routinely appear when a new communicant joins a chat.[20]

13. If implemented, these measures would pose serious threats to digital security,[21] by undermining authentication systems, by introducing potential unintentional vulnerabilities, and by increasing risks that communications systems could be abused or misused.[22] More importantly, any obligation imposed upon communications services providers to decode encrypted communications forces the creation of software back-doors which, once found, can be easily exploited by both legitimate and criminal actors. As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlighted in the 2015 report:

> It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.[23]

14. This Court has repeatedly held that "*Article 8 protects, inter alia, the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world*" (*Breyer v. Germany*, App. No. 50001/12, §73). In *Barbulescu v. Romania* (App. No. 61496/08), the Grand Chamber of this Court affirmed that the broad interpretation given to the notion of private life ought to encompass "*the right to lead a "private social life", that is, the possibility for the individual to develop his or her social identity*" (§70). It is also the established case-law of this Court that "*[t]apping and other forms of interception*

---

[19] Paul Szoldra, ISIS' favorite messaging app may be in jeopardy (Business Insider, 28 June 2016), https://www.businessinsider.com/russia-anti-encryption-telegram-2016-6?r=US&IR=T.

[20] PI, Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages.

[21] Davis, Terry/Peha, Jon M./Burger, Eric William/Camp, L. Jean/Lubar, Dan, 'Risking it All: Unlocking the Backdoor to the Nation's Cybersecurity' (2014), https://ssrn.com/abstract=2468604.

[22] PI, FREAKShow: Why governments meddling with encryption standards hurts us all (5 March 2015), https://privacyinternational.org/blog/1482/freakshow-why-governments-meddling-encryption-standards-hurts-us-all.

[23] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32, 22 May 2015).

of telephone conversations represent a serious interference with private life and correspondence" (*Kruslin v. France*, App. No. 11801/85, § 33; *Huvig v. France*, App. No. 11105/84, § 32; *Kopp v. Switzerland*, App. No. 23224/94, § 72).

15. Considering the vital role encryption plays for individuals' modern communications[24] and the risks inherent in the measures that seek to undermine it, PI submits that an order requiring a communications services provider to provide the means for decoding encrypted messages constitutes a serious interference with Article 8 of the Convention. The Intervener also submits that, as the Court has rightly held, novel surveillance techniques, such as those that seek to decode encrypted communications, must be "*accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*" (*Szabó and Vissy v. Hungary*, App. No. 37138/14, § 68).

IV. By obliging communication services providers to actively provide means to decode encrypted communications, a state violates its positive obligations under the Convention

16. In order to comply with an obligation to retain encrypted messages for a certain time and be able to effectively decrypt them, communication services providers would have to make radical changes to their infrastructure and code.[25] The latter will undoubtedly undermine the existing encryption tools offered (by modifying or removing provisions for forward secrecy) by these providers and compromise the level of security offered to individuals. This is because these changes, which, in the case of end-to-end encrypted communications, for example, will allow providers to obtain access – for the first time – and, without notifying users, to secretly insert a third party to existing and future communications, would have to be implemented in the form of a software update that indiscriminately targets all users of the application or service in question.[26] In other words, the only way for a communication services provider to be able to store and hand over encrypted messages in a way that can be decoded would be to pre-emptively insert a 'secret' third participant in all existing and future conversations between users and retain their correspondence until the retention period imposed upon them has elapsed.

17. As explained above, for messaging applications to be able to suppress notifications when a ghost user is added, service providers would need to rewrite the software that every user relies on. This means that any mistake made in the development of this new function could create an unintentional vulnerability that affects every single user of that application.[27] As security researcher Susan Landau points out, this "*involves changing how the encryption keys are negotiated in order to accommodate the silent listener, and that means creating a*

---

[24] According to a 2016 Flash Eurobarometer survey by the European Commission, an overwhelming majority of 90% of people in the European Union agree that "*they should be able to encrypt their messages and calls, so they are only read by the recipient*", page 43, https://europa.eu/eurobarometer/surveys/detail/2124.

[25] Nate Cardozo/Seth Schoen, Detecting Ghosts by Reverse Engineering: Who Ya Gonna Call? (EFF, 23 January 2019), https://www.eff.org/deeplinks/2019/01/detecting-ghosts-reverse-engineering-who-ya-gonna-call.

[26] Matthew Green, On Ghost Users and Messaging Backdoors (17 December 2018), https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors.

[27] PI, Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages.

much more complex protocol —raising the risk of an error".[28] A look back at recent news stories on unintentional vulnerabilities that are discovered in encrypted messaging apps like iMessage,[29] and devices ranging from the iPhone[30] to smartphones that run Google's Android operating system,[31] lend credence to her concerns. Any such unintentional vulnerability would ultimately open a Pandora's box of potential exploitation by malicious third parties.

18. Article 8 of the Convention does not only impose negative but "*may also impose on the State certain positive obligations to ensure effective respect for the rights protected*" by it (see, inter alia, *X and Y v. the Netherlands*, App. No. 8978/80, § 23; *Von Hannover (no. 2)*, App. Nos. 40660/08 60641/08, § 98; *Hämäläinen v. Finland*, App. No. 37359/09, § 62). While this Court had recognised that states enjoy a certain margin of appreciation in choosing how to realise the protections enshrined in Article 8, their discretion is not unlimited, especially in a field such as communications surveillance where the potential for abuse is extremely high (*Klass and Others v. Germany*, App. No. 5029/71, § 50; *Roman Zakharov v. Russia*, App. No. 47143/06, §§ 232-34). In *Barbulescu*, which concerned the monitoring of an employee's communications by his employer, the Grand Chamber held that "*domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake*" (§ 141). In finding that there had been a violation of Article 8 of the Convention, the Grand Chamber placed particular emphasis on the proportionality of the surveillance measures undertaken by the employer, the fact that the "*monitoring of the content of communications is by nature a distinctly more invasive method*" which "*requires weightier justification*", as well as on the international and European law in this area (§ 121).

19. In that regard, it should be underlined that European Union (EU) law imposes a series of obligations on states to guarantee the privacy and confidentiality of communications, as well as the security and integrity of information technology systems.[32] In particular, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 establishes rules for the processing of personal data, also in the context of a criminal investigation.[33] Among

---

[28] Susan Landau, Exceptional Access: The Devil is in the Details (Lawfare, 26 December 2018), https://www.lawfareblog.com/exceptional-access-devil-details-0.

[29] Ellen Nakashima, 'Johns Hopkins Researchers Poke a Hole in Apple's Encryption' (Washington Post, 21 March 2016), https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccdbc5f74e_story.html?utm_term=.2485b9a99233.

[30] Lorenzo Franceschi-Bicchierai/Joseph Cox, 'The Cat-and-Mouse Game Between Apple and the Manufacturer of an iPhone Unlocking Tool' (VICE Motherboard, 18 April 2018), https://motherboard.vice.com/en_us/article/ne95pg/apple-iphone-unlocking-tool-graykey-cat-and-mouse-game.

[31] Brian Barrett, 'Millions of Android Devices are Vulnerable Right Out of the Box' (Wired, 10 August 2018), https://www.wired.com/story/android-smartphones-vulnerable-out-of-the-box.

[32] See, inter alia, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981, ETS no. 108); Charter of Fundamental Rights of the European Union (2007/C 303/01); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.

[33] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

others, the Directive underlines a series of obligations for law enforcement authorities to ensure the security, integrity and confidentiality of personal data by implementing relevant measures.[34] Finally, the EU Directive on security of network and information systems (the NIS Directive) provides legal measures to boost the overall level of cybersecurity among member states.[35]

20. As individuals continue to integrate online communications into the fabric of their lives, economies and societies,[36] safeguarding the security of communications infrastructure and services becomes increasingly important.[37,38] Contrary to these obligations, in order to retain and be able to decode encrypted communications, communication services providers would have to fundamentally implement changes to their communication services, by creating software back-doors, for instance, that would affect all users indiscriminately and, consequently allow for the unlawful exploitation of their data at a large scale.

21. The Intervener submits that, under these circumstances, requesting the implementation of measures requiring the retention and decoding of encrypted communications contradicts the national authorities' obligations to guarantee the confidentiality and privacy of communications, as well as the security and integrity of information technology systems. By their very nature, measures that seek to weaken encryption require the exact opposite, a continuous undermining of security.

V. Measures obliging telecommunication services providers to create software back-doors for the indiscriminate retention and decoding of encrypted communications cannot be limited to what is "necessary in a democratic society"

22. As discussed above, the implementation of measures by communications service providers to indiscriminately retain and facilitate access to encrypted communications, such as those examined by the Court in the present case, would require the latter to alter their existing services by creating back-doors, such as inserting 'silent listeners' to conversations, so that they can be able to retrospectively access the encrypted messages that have been retained. As this cannot be targeted to specific users, which might, for instance, present a threat to national security or serious crime, the implementation of these measures would have to indiscriminately affect everyone. In other words, the creation of backdoors to comply with government measures that seek to weaken encryption directly implies a severe compromise of millions or billions of users of that service. This is because "*a backdoor is a technical capability —a vulnerability—that is available to anyone who knows about it and has access*

---

[34] Ibid, Article 29 (Security of processing).
[35] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194.
[36] According to a 2016 Flash Eurobarometer survey by the European Commission, an overwhelming majority of 90% of people in the European Union agree that "*they should be able to encrypt their messages and calls, so they are only read by the recipient*", page 43, https://europa.eu/eurobarometer/surveys/detail/2124.
[37] See Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Expert report of Professor Ross Anderson (30 September 2015), pages 17-19, https://privacyinternational.org/sites/default/files/2018-03/2015.09.30%20Anderson_IPT_Expert_Report_2015_Final.pdf.
[38] Ibid, Witness Statement of Eric King (5 October 2015), pages 22 ff, https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf.

to it".[39] Therefore, introducing changes to allow for complex new exceptional access requirements will inevitably increase the security flaws lurking in the software infrastructure for decades to come.[40]

23. The possibility of security flaws designed to give exceptional access to law enforcement being exploited by hostile actors is far from theoretical.[41] Between 1996 and 2006, it appears that insiders at Telecom Italia enabled the wiretapping of 6,000 people, including business, financial, and political leaders, judges, and journalists.[42] From 2004 to 2005, the cell phones of 100 senior members of the Greek government, including the Prime Minister, the head of the Ministry of National Defence, the head of the Ministry of Justice, and others were wiretapped by unknown parties through lawful access built into a telephone switch owned by Vodafone Greece.[43] Similar vulnerabilities have also been exploited by third parties with onerous consequences for millions of individuals globally. WannaCry, for example, was developed by hackers who effectively managed to exploit software vulnerabilities stockpiled by the United States National Security Agency (NSA),[44] and seriously impacted European infrastructure operators in the sectors of health, energy, transport, finance, and telecoms.[45]

24. International human rights laws require that any interference with privacy rights must be necessary and proportionate. These principles were authoritatively confirmed in the recent UN Human Rights Council resolution on the right to privacy in the digital age, which also "*calls upon States not to interfere with the use of [encryption] thereon complying with States' obligations under international human rights law, and to enact policies that protect the privacy of individuals' digital communications*".[46] In the 2015 report to the UN Human Rights Council on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recommended:

> States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate.[47]

---

[39] Bruce Schneier, Evaluating the GCHQ Exceptional Access Proposal (Lawfare, 17 January 2019), https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal.

[40] Harold Abelson/Ross Anderson/Steven M. Bellovin/Josh Benaloh/Matt Blaze/Whitfield Diffie/John Gilmore/Matthew Green/Susan Landau/Peter G. Neumann/Ronald L. Rivest/Jeffrey I. Schiller/Bruce Schneier/Michael Specter/Daniel J. Weitzner, 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', Computer Science and Artificial Intelligence Laboratory Technical Report (MIT-CSAIL-TR-2015-026, 6 July 2015).

[41] For a recent list of examples of how software security flaws can be exploited across the globe, see PI, Backdoors, https://privacyinternational.org/examples/backdoors.

[42] Piero Colaprico, '"Da Telecom dossier sui Ds" Mancini parla dei politici' (La Repubblica, 26 January 2007), http://www.repubblica.it/2006/12/sezioni/cronaca/sismi-mancini-6/dossier-ds/dossier-ds.html.

[43] V. Prevelakis and D. Spinellis, 'The athens affair' (Spectrum, IEEE, Vol. 44, No. 7, 2007), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4263124.

[44] Zack Whittaker, 'Two years after WannaCry, a million computers remain at risk' (TechCrunch, 12 May 2019), https://techcrunch.com/2019/05/12/wannacry-two-years-on.

[45] EU Agency for Fundamental Rights (FRA), Fundamental Rights Report 2018, page 161, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

[46] Resolution on the Right to Privacy in the Digital Age, A/HRC/48/L.9/Rev.1, 7 October 2021.

[47] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32, 22 May 2015), para 60.

25. This Court has applied 'strict necessity' to interferences with the right to privacy in the surveillance context. In *Szabó and Vissy*, it indicated that, given "*the potential of cutting-edge surveillance technologies to invade citizens' privacy, … any measure of secret surveillance which does not correspond to [strict necessity requirements] will be prone to abuse*" (§ 73). In addition, when determining whether an interference with the right to privacy was "*necessary in a democratic society*", the Court examines whether that interference was proportionate to the aims pursued. This necessarily involves a balancing exercise between competing interests (*Z v. Finland*, App. No. 22009/93, § 94).

26. This Court has recognised on numerous occasions that blanket or indiscriminate measures that seriously interfere with privacy may not be justified. In *S. and Marper v. the United Kingdom* (App. Nos. 30562/04 and 30566/04), the Grand Chamber held that the collection and retention of DNA and fingerprints of innocent people was contrary to Article 8. In particular, the Grand Chamber was "*struck by the blanket and indiscriminate nature of the power of retention in England and Wales*" (§ 119), concluding that "*the blanket and indiscriminate nature of the powers of retention…fails to strike a fair balance between the competing public and private interests*" (§ 125). It held that the UK had "*overstepped any acceptable margin of appreciation in this regard*" even though the DNA database was undoubtedly a valuable tool for detecting and prosecuting serious criminals (§ 125).

27. In light of the above, the Intervener submits that measures requiring communication services providers to facilitate the blanket retention and decoding of encrypted communications are not compatible with Article 8 of the Convention as they constitute a serious interference with the right to privacy and are not limited to what is "*necessary in a democratic society*".

London, 6 December 2021

On behalf of the Intervener

Ioannis Kouvakas

Legal Officer and Acting General Counsel

Privacy International