No Backdoor for Mass Surveillance

The European Court of Human Rights Protects the Right to Encrypted Communication

Erik Tuchtfeld

29.02.2024 doi: 10.59704/8939c7915eda51dc

Bulk data retention is the evergreen of European security policy. On February 13, the European Court of Human Rights (ECtHR) – once again – ruled in Podchasov on Russia's collection of and access to citizens' private communication. In the midst of the ongoing debate about the alleged dangers of encrypted communications, leaving law enforcement authorities "in the dark", the Court made it clear that weakening the encryption of all citizens cannot be justified. This sends an important message not only to the Russian state, but also to other European governments that contemplate installing "backdoors" on encrypted messenger services like Telegram, Signal or WhatsApp.

Although the Court passed up the opportunity to make a general ruling on the legality of blanket data retention of communications content, it did emphasize its procedural approach and found that the lack of legal safeguards for access to communications data violated the right to privacy.

The Procedural Difficulties of a Divorce

Some may wonder why the Court still has jurisdiction in cases concerning Russia. Russia was expelled from the Council of Europe on March 16, 2022, following its illegal invasion of Ukraine, and, six months later, ceased to be a Party to the European Convention on Human Rights. However, as the Convention bound the Russian state until September 16, 2022, all cases relating to actions of the state up to this date remain admissible to the Court. This includes the 17,450 applications against Russia that were pending on September 16, but could even lead to new applications as long as they concern actions before September 16, 2022 (see para. 35). The present case, for example, was filed on June 18, 2019.

The Matters at Stake

Russian legislation requires "Internet communication organizers" (ICO) to store all communication data (metadata, such as timestamps and the sender and recipient of a message) generated by Russian internet users for one year and the contents of all communications for six months. If communications are encrypted, ICOs must provide all information necessary to decrypt them (paras. 19-20). In addition, ICOs must provide the Federal Security Service (FSB) with 24-hour remote access to the content and metadata of the communications they process (para. 26).

The applicant is a user of the messenger Telegram. While Telegram's chats are generally not end-to-end encrypted, its so-called "secret chats" are. In 2017, the FSB asked Telegram to provide information to decrypt the communications of six Telegram users that had taken place in "secret chats". Telegram argued that it was technically impossible to provide information to decrypt the messages without installing a general backdoor that would allow the decryption of all its users' communications. It was later fined by the Meshchanskiy District Court (paras. 7-8). The Taganskiy District Court of Moscow even ordered the blocking of Telegram in Russia due to this "noncompliance", resulting in bizarre collateral damages as more than 19 million IP addresses were blocked, and many unrelated services became unreachable. Telegram was blocked for over two years. Having been unsuccessful in challenging the orders in Russia, it lodged a currently pending application before the ECtHR (a case that is likely to rely heavily on Podchasov).

The Court's Failure to Judge on Bulk Data Retention

In the present case the Court had to assess three different, albeit related, interferences with the applicant's rights: First, the general bulk retention of personal communication data. Second, the FSB's possibilities to access it with little to no judicial restraint. Third, the more specific problem of access to end-to-end encrypted communications, including the requirement to release decryption keys.

The Court, however, decided that the legality of bulk data retention did not need to be assessed on its own. To recap, the Russian legislation obliges ICOs to retain all metadata for one year and all content of online communications for six months. This goes far beyond the scope of the mere retention of metadata (including IP addresses, timestamps, participants of communication etc., but not the content) provided for by former legislation in the European Union, which was struck down by the European Union's Court of Justice due to its incompatibility with fundamental rights several times (Digital Rights, 2014; Tele2 Sverige AB, 2016; Commissioner of the Garda Síochána, 2020; La Quadrature du Net, 2020; SpaceNet, 2022). This jurisprudence was explicitly acknowledged by the ECtHR (para. 31). The Court also stressed that "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [...] irrespective of whether the retained data were then accessed by the authorities" (paras. 51-52). Thus, it remains irritating and methodologically unconvincing that it decided to remain "struck by the extremely broad duty of retention provided by the contested legislation" (para. 70), leaving the legality of said interference open and only examined "with particular attention [... the] safeguards against abuse relating to the access by the law-enforcement authorities" (para. 71). While this is an approach taken by the Court in the past (see, for example, Ekimdzhiev, paras. 372, 385 et seq.), the particular severity of Russia's data retention regime was an open invitation to evaluate the data retention on its own, not only in relation to the safeguards in place (this reluctance already shown in Big Brother Watch to assess the actual substance of data retention has been described by Monika Zalnieriute as "procedural fetishism"). The approach is all the more surprising as only two days later, in Škoberne (paras. 139-146), another chamber of the Court – referring heavily to ECJ jurisprudence – classified mass (meta-)data retention as such as unlawful.

However, the second – and in my view separate – question of sufficient safeguards was quickly answered by the Court. It highlighted that the safeguards in question were "the same legal regime which was examined in Roman Zakharov [where] the Court found that Russian legal provisions governing secret surveillance measures did not meet the 'quality of law' requirement because they did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse" (para. 74). Put simply, a broad description of the purposes for which the authorities may access communications data (ranging from the prevention of crime to economic security), permanent remote access, and the refusal to provide the ICOs with supposedly existing court orders are not sufficient to justify interferences in a democratic society. The impression the Court's judgement left on the Russian institutions back then is shown by the reaction of the Russian parliament. On the same day in December 2015, the Duma passed a new law allowing the constitutional court to overrule ECtHR judgments that contradict the Russian constitution.

End-To-End May Be Your Friend

The third, and groundbreakingly new aspect of the case was the obligation for communication services to provide access to end-to-end-encrypted communications.

Not all digital communications services use end-to-end encryption. For example, e-mails (and Telegram chats that are not explicitly marked as "secret chats") are in most cases only transport-encrypted. This means that the content is encrypted during the transport (e.g. from the sender's device to their e-mail server, and from there to their Russian colleague's e-mail server) but it is stored on the respective servers in a decrypted state. As a result, the sender's e-mail

provider and the e-mail provider of the recipient have access to the actual content of the messages and are de facto able to release them to law enforcement.

This is not the case with end-to-end encrypted communication. The two "ends" in this term are generally understood to be the respective devices of the communication participants. For example, when one uses WhatsApp or Signal (two messengers supporting end-to-end encryption in all their chats) to send a message to a colleague, the message is encrypted on their device, transmitted through a variety of countries in this encrypted state (making it total gibberish to anyone who might intercept it in between) and only decrypted on the recipient's device. Thus, not even the messenger service itself has access to the content of that message (it might only, still, have access to the metadata).

Since the messenger is unable to access the content of the message, it cannot release it to law enforcement authorities. Now, one could argue, this must be the end of the story. Already the old Romans knew that "impossibilium nulla est obligatio" ("the impossible can't be an obligation"). No access to the content means no possibility of releasing it means no obligation.

Targeted Measures Must Not Affect Everybody

Unfortunately, the law enforcement authorities in Russia (and beyond) are not satisfied with this result. They asked Telegram for the keys to decrypt the suspects' communication. Telegram was unable to provide them as the keys are not in the hands (more precisely: stored on the servers) of Telegram, but on the devices of the suspects. Telegram could only give third parties access to the keys by updating its application for all users, adding a "backdoor" that would extract the private key from the device and send it to law enforcement authorities.

Such a measure, as the Court rightly points out, would "make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications [...,] may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications" (para. 77). As it weakens the encryption for all users, it is not proportionate, and violates the applicant's right to privacy under Article 8 ECHR.

A Call for Europe

The Court emphasizes the importance of end-to-end encryption not only for the enjoyment of the right to privacy, but also for freedom of expression, and as a protection against abusive actions, such as hacking, identity theft, and the disclosure of confidential information. It is a statement made not only for the ears of the Russian government, but for governments across Europe. Encrypted communication has been a thorn in the side of law enforcement authorities for decades.

In 2022, the European Commission proposed mandating messengers to scan all private communication for potentially illegal content. Messaging services using end-to-end encryption would be required to scan the content on the device before it gets encrypted ("client-side-scanning"). While the legislative process on the current proposal (the so-called "CSAM regulation") appears to have stalled for now, the EU has set up a high-level working group on the phenomenon of "going dark". The concept is used to describe the increasing use of encrypted chats by suspects, allegedly leading to law enforcement becoming "blind" and stopping them from effectively protecting the public.

One can only hope that this working group will read the judgment as a call to consider "alternative methods of investigation", as the Court puts it (para. 78), that are in line with fundamental rights. For decades, security laws enabling mass surveillance of citizens have been struck down by courts across Europe. The political focus of law enforcement on these measures has diverted resources that could have been spent on effective and long-term solutions to crime that are compliant with human rights. Instead, illegal mass surveillance has made Europe a less safe place.

ABOUT THE AUTHOR

Erik Tuchtfeld
Erik Tuchtfeld is a Research Fellow at the Max Planck Institute for Comparative Public Law and International Law in Heidelberg, where he heads the humanet3 group. He is an Associate Editor at Verfassungsblog.

SUGGESTED CITATION

Tuchtfeld, Erik: No Backdoor for Mass Surveillance: The European Court of Human Rights Protects the Right to Encrypted Communication, Verfassungsblog, 29.02.2024, doi: 10.59704/8939c7915eda51dc.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20240229-105220-0.