Letter to the Council of the European Union, the German Federal Ministry of the Interior and the Federal Ministry of Justice

17 November 2020

Do not break the encryption of messenger services!

Dear members of the Council of the European Union,

In light of the recent terror attacks, the German presidency of the Council of the EU has put forward a draft resolution[1] that calls for “technical solutions” to enable access to encrypted communications for “competent authorities in the area of security and criminal justice”. We are writing to you to express our concern over the pursuit of a regulatory framework that would call into question the integrity of end-to-end encrypted messenger services and thereby endanger the right to privacy and the confidentiality of the communication of journalists and their sources.

The so-called "security through Encryption and security despite encryption" is a contradiction in itself. Encryption either works without exception, or it does not work at all. A functioning encryption with an exception only for EU intelligence and police services is not conceivable and not possible. Any technical means to access encrypted communication would severely weaken the confidentiality of all users’ data, leaving citizens and services at a heightened risk of attacks by bad faith actors, even if the proposed solution were to comply with “the principles of legality, transparency, necessity, and proportionality”.

It is to be feared that the access to data envisaged by the draft resolution would mean the creation of backdoors for "competent authorities", through which authorities would be able to access and read citizens’ communication. “Competent authorities" does not only mean criminal investigators but appears to include secret services as well. A backdoor would give these services the possibility to not only access and save individual chats of a few people, but to intercept the communication stream of all users of messenger services.

If this were to be implemented, it would endanger journalists’ ability to protect the confidentiality of their communications and the identities of their sources. End-to-end encrypted messengers are an essential research and communication tool for journalists in the digital age that must not be compromised. The essential control function of journalism as an independent watchdog in a democracy depends upon the ability of journalists to communicate safely and in full confidentiality.

It appears the attack in Vienna could only happen because the secret service in Austria failed to use readily available information on the attacker. Not more surveillance powers, but better work by the authorities might have prevented the attack. The very authorities whose failure allegedly made the attack possible in the first place are now to be given even more competences.

We therefore call upon the European Council, the Federal Ministry of the Interior and the Federal Ministry of Justice not to pursue any efforts that might jeopardize citizens’ right to privacy. Preserving end-to-end encryption is crucial to the protection of human rights and

[1] Draft Council Resolution on Encryption - Security through encryption and security despite encryption https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf

press freedom. Any further discussions should be conducted in a transparent and open manner and include civil society representatives.

Sincerely,

Christian Mihr

Reporter ohne Grenzen

Julia Stein

Netzwerk Recherche