Council of the
European Union

Brussels, 30 June 2022
(OR. en)

10792/22

INF 109
API 49

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Public access to documents - Confirmatory application No 07/c/01/22

Delegations will find attached:

- the request for access to documents sent to the General Secretariat of the Council on 14 June 2022 and registered on the same day (Annex 1);
- the reply from the General Secretariat of the Council dated 28 June 2022 (Annex 2);
- the confirmatory application dated 28 June 2022 and registered on the same day (Annex 3).

ANNEX 1

[E-mail message sent to access@consilium.europa.eu on Tuesday 14 June, 2022 12:42]

From: **DELETED**

Sent: Tuesday, June 14, 2022 12:42 PM

To: TRANSPARENCY Access to documents (COMM) <Access@consilium.europa.eu>

Subject: Access request to a document

Hello

Can I get a copy of the document 7675/20, including all its annexes?

Best regards

DELETED

Council of the European Union
General Secretariat
Directorate-General Communication and Information - COMM
Directorate Information and Outreach
Information Services Unit / Transparency
Head of Unit

Brussels, 28 June 2022

DELETED
Email: **DELETED**

Ref. 22/1291-rh/ns

Request made on: 14.06.2022

Dear **DELETED**,

Thank you for your request for access to documents of the Council of the European Union.[1]

I regret to inform you that access to documents **7675/20** and **7675/20 ADD 1** cannot be given for the reasons set out below.

Documents **7675/20** and **7675/20 ADD 1** of 8 May 2020 are notes from EU Counter-Terrorism Coordinator to delegations on law enforcement and judicial aspects of encryption. They contain policy making considerations on a very sensitive topic, which is still under discussion in the EU bodies and beyond.

[1] The General Secretariat of the Council has examined your request on the basis of the applicable rules: Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43) and the specific provisions concerning public access to Council documents set out in Annex II to the Council's Rules of Procedure (Council Decision No 2009/937/EU, OJ L 325, 11.12.2009, p. 35).

The objective of these documents is to serve as a basis for discussion with experts. The documents are still undergoing examination in the Council. For the Council to reach an agreement, its Member States held consultations and exploratory talks. To reveal the content of such talks before a common position has been reached would interfere with the negotiations and would jeopardise the conclusion of an agreement within the Council.

The disclosure of the texts at a moment when the appropriate balance of the various interests involved has not yet been achieved within the Council's preparatory bodies would reduce the flexibility for delegations to formulate and reconsider their positions in the light of the arguments exchange in the debate. This would seriously affect the chances of finding a convergence in delegations' positions.

Disclosure of the documents at this stage would therefore seriously undermine the decision-making process of the Council. As a consequence, the General Secretariat has to refuse access to these documents.[2]

Having examined the context in which the documents were drafted, on balance the General Secretariat could not identify any evidence suggesting an overriding public interest in their disclosure.

We have also looked into the possibility of releasing parts of the documents.[3] However, as the information contained in the documents forms an inseparable whole, the General Secretariat is unable to give partial access.

Pursuant to Article 7(2) of Regulation (EC) No 1049/2001, you may ask the Council to review this decision within 15 working days of receiving this reply. Should you see the need for such a review, you are invited to indicate the reasons thereof.

Yours sincerely,

Fernando FLORINDO

[2] Article 4(3), first subparagraph, of Regulation (EC) No 1049/2001.
[3] Article 4(6) of Regulation (EC) No 1049/2001.

ANNEX 3

[E-mail message sent to access@consilium.europa.eu on Tuesday, June 28, 2022 11:45]

From: **DELETED**

Sent: Tuesday, June 28, 2022 11:45 AM

To: TRANSPARENCY Access to documents (COMM) <Access@consilium.europa.eu>

Subject: Re: Ref. 22/1291-rh/ns

Dear Mr Florindo

I thank you for your response (22/1291-rh/ns).

You can find the request to review your decision, and the reasons thereof, as an attachment.

I do not wish my name (or other personal information) to be made available to the public at this point in time.

Best regards

DELETED

Access to documents concerning the debate on encryption
28.6.22

Dear Mr Florindo

I thank you for your response (22/1291-rh/ns).
In this text I will demand to have full access to the document 7675/20 and all of its annexes. These specific demands will be made at the end of this text.
But before that, I will justify the demands with the following arguments.
The topic of encryption, and especially the debate related to so called 'lawful access to encrypted material', is of utmost importance to civil society, national security, the future of democracy worldwide and the future of the European Union.
Even though we are already highly dependent on information technology, information technology will become ever more pervasive and transformative through emerging technologies such as augmented and virtual reality, blockchain technologies and services built on top of them, artificial intelligence, other kinds of new digital services, robots and autonomous vehicles.
Thus we are currently living the beginnings of the Information Age. In fact, we are living in the Dark Ages of the Information Age, and are decades away from the Age of Enlightenment. This claim is easily justified by the facts that, in our day and age: 1) unacceptably sensitive and large-scale data breaches and hacks are continually happening, 2) digital services, file storage services and cloud-based collaboration services and social media platforms are largely provided by a few US-based corporations, thus centralizing collected data, internet traffic and content filtering capabilities to these entities and to the US itself 3) computer science is not a mandatory subject in schools and it is also not taught to the adult population, making 99% of the world's population *digitally illiterate* and 4) mass surveillance is pervasive.
Regarding mass surveillance, there are several intergovernmental organizations that have made statements condemning mass surveillance, or have expressed being deeply concerned about it. For example the *Parliamentary Assembly of the Council of Europe* has condemned mass surveillance and attempts to weaken encryption standards in their resolution 2045 from the year 2015. The *UN* has expressed in their Resolution 73/19 (*The right to privacy in the digital age*) deep concern about the negative impact of surveillance (especially when carried out on a mass scale).

In their groundbreaking decision in 2020, the CJEU invalidated the EU-US Privacy Shield agreement, basing their decision on US surveillance laws being in contradiction with fundamental rights. Mass surveillance also continues to be actively discussed topic: it was for example discussed in the *Internet Governance Forum 2020* (which was a two week event organized by the *UN*).

What makes mass surveillance possible? There are several factors, of which we shall list a few. One technical factor is the fact that digital services and data storage are largely centralized (they are provided by a few US-based corporations). Another factor is the general political climate which attempts to silence critics by employing *dangerous rhetoric*, by using statements such as 'nothing to hide, nothing to fear'. Third factor which makes mass surveillance possible, is the large-scale usage of devices and software whose designs and source codes are secret information.

Let's talk a bit about this last point.

Currently, the designs of the physical components of our devices, such as smartphones, personal computers and server computers, are practically secret information. The designs are in practice only known by the manufacturers and designers of these devices. The source codes of the software that we run on our devices are also largely secret information. The consequence of these designs and source codes being secret information is, that analyzing the behaviour of our devices is so resource intensive for computer security experts, that it is not possible to have any reasonable assurances about what our devices actually do, what data they collect, where they send this data or whether they contain any backdoors or not.

Now, talking only about mass surveillance is highly misleading, since the same ecosystem and technical capabilities that enable mass surveillance, can be used as well:

- To conduct global-scale censorship in digital services such as email, social media platforms and instant messaging services.
- To surreptitiously subject people to algorithmically and automatically targeted political and ideological content on social media platforms, video sharing services and search engines through the use of recommender systems.
- To conduct offensive and targeted hacking of electronic devices.

From the perspective of fundamental rights, democracy and national security, this is obviously a completely unacceptable state of affairs. The situation is even more unacceptable, when we consider the fact that in a few years, we shall have large autonomous devices roaming around in factories and in the streets that have actual *dynamic physical presence*: robots and autonomous vehicles. For example these robots, autonomous vehicles and the devices that are used to control them remotely, *must not contain any backdoors* (intentional security weaknesses) that any government agency (foreign or domestic), extremist group or hacker group could abuse to injure people or get them killed.

The threat of the current information technology and digital service ecosystem to democracy is real. We must work towards securing and hardening our systems, not making them any weaker than they already are. *One required component* for securing our data, communications, our systems and fundamental rights, is the use of encryption. We must embrace strong and non-backdoored encryption on all levels of the hardware and software stack.

Thus it is highly worrying, that for example EU's Counter-Terrorism Coordinator Gilles de Kerchove appears to be openly quite hostile towards encryption, as seems to be demonstrated by his reaction (the reaction can be found under the *Current reactions* heading, and is visible at least on the date 22.12.20) to the *International Statement: End-ToEnd Encryption and Public Safety* and especially by his views expressed on the Council of the European Union document 7675/20.

There are other aspects in the discussion that are worrying as well. For example based on some of the EU's documents discussing these issues, there seems to be technical misunderstandings about how encryption works, and additionally these documents contain other encryption related technical mistakes. Also the concept of 'end-to-end encryption' is often mischaracterized in these documents.

The current encryption systems in place and their usage are already wholly inadequate as they are, for securing democracy, fundamental rights, national security and our future. Weakening encryption or building backdoor access capabilities is not a solution.

All efforts to install backdoors into the encryption components of software, hardware and digital services for gaining 'lawful access' to encrypted data, or to weaken their authenticity, confidentiality and privacy guarantees, must be considered dangerous per se. Citizens must have *radical transparency* into the decision making process, into the deliberations, into the level of discussion, into the amount of lobbying and into the amount of technical misunderstandings, so that citizens can attempt to participate in the debate, influence the decision making and in general participate in the democratic process.

For all of these reasons, I demand that you provide me the full copy of the document 7675/20 and all of its annexes. In addition to these, I demand that you provide me any other internal documents containing deliberations and preliminary consultations regarding this particular issue of encryption.

Best regards

DELETED