Netherlands

Subject: response to EC working-paper on data retention (WK 7294/2021 INIT)

The views expressed here are preliminary views and may not in any circumstances be regarded as stating an official position of the Dutch government.

Policy approach 1: no EU initiative

Question: Do Member States see merits or drawbacks in maintaining a national approach to data retention legislative measures?

The Netherlands is - as was mentioned on multiple occasions by the Dutch Minister of Justice and Security, like in the JHA council meeting of March 2021 - in favour of new EU legislative instrument on data retention, so that a useful and legally sustainable data retention obligation is applied in a uniform manner in all Member States. The drawbacks of 26 national legal frameworks for data retention are manifold, like:

- Legal uncertainty for EU citizens. Depending on the (visited) country, more or less data is retained.
- Each MS has a (very) different legal framework, which will most likely lead to more future cases before the CJEU, and prevent the creation of a long-term stable legal basis.
- It creates difficulties for cross-border criminal investigations, because of too many differences in data retention regimes in the various Member States.
- It creates uncertainty for (international) providers.

Policy approach 2: Non-regulatory initiative on data retention

Question: Do Member States consider this a viable way forward?

This approach could be investigated as an alternative if approach 3 – an EU legal framework – is not feasible. This approach will create some basis for MS to create a national law, but will most likely not entirely mitigate the problems identified under approach nr.1.

Policy approach 3: regulatory initiative on data retention

Question: Could Member States consider a 'mixed' approach of both national and EU measures? If so, what aspects should be regulated at which level (EU or national)?

This approach merits further detailed discussion, and could potentially be considered. NL would favour an approach whereby an EU instrument would lay down a general legal framework for national data retention regimes. Preliminary thoughts on this are that the EU framework determines for which purposes data may be retained, lays down what categories of data may be retained so that only data is retained which is strictly necessary for that purpose, sets a range (or maximum) for the term that telecommunications data may be retained and provides that retained data may only be stored and processed in the territories of the EU Member States. Issues concerning access and procedural conditions – how data is stored, which authorities may grant access, etc. – will be left to national regulation.

Approach 3(a): generalised retention of traffic and location data for national security purposes
Questions: In light of the delineation of national and EU competences, what are Member States' views on a legislative initiative that would harmonise certain criteria relating to the retention of traffic and location data and related access conditions for national security purposes, for situations that involve private actors (for storage, transmission and providing access to data to relevant competent authorities)?

The Netherlands considers national security matters - laws and activities - to fall outside of the competence of the EU.

Approach 3(b): targeted data retention of traffic and location data for serious crime and serious threats to public security (and, a fortiori, safeguarding national security)
Questions: What are the legal challenges for Member States and the technical challenges for providers to comply with a targeted retention obligation and how could they be overcome? Please be as specific and concrete as possible in your responses. What is the 'objective evidence' (in the case of persons) and what are the 'objective and non-discriminatory factors' (in the case of geographical areas) or other objective criteria that Member States could consider in drawing up a targeted retention framework?

This option needs further investigation. Based on our first analysis there are many judicial and technical challenges - and they may be too great - to implement an effective (useful for LEA and technically manageable for providers) and legally correct (non-discriminatory) targeted retention scheme. We have not found ways to overcome them. These challenges include:

- Criminals will avoid locations where data is retained.
- Serious crime occurs everywhere and in all circles of the population. It simply cannot be predicted which individuals - perpetrators and victims - are involved in a criminal offense during what period and location. Nor can it be predicted which means of communication are used.
- Many forms of (organised) crime cannot be geographically defined, because location changes are part of the concealment strategy.
- Targeted retention will most likely not work for retaining meta data of (potential) perpetrators of crimes like cybercrime or cyber enabled crime.
- Providers cannot easily cut off retention at the boundary of a geographical location. An antenna does not follow geographical areas exactly.
- Pre-differentiating to a particular circle of persons or a particular geographical area potentially leads to stigmatisation and possibly discrimination. Think, for example, of a retention obligation for a certain population group or district that comes into contact with crime a lot.
- For OTT services it is not always possible or legally permissible to determine the location of a user in order to decide if the users data should be retained because the user is within a geographical retention zone.

The view of the Netherlands is that it is more a theoretical than practical option, but, as mentioned, it would be interesting to further (empirically) investigate its operational potential. For example to examine the experiences in practice of the MS that have implemented a targeted retention scheme,

or are planning to do so, like Belgium and France. We are not aware of any practical experience at this time.

Question: Do Member States consider there is merit in revisiting the 'data matrix' exercise initiated by Europol in 2018 to try to find ways to devise a targeted retention system that fulfils the Court's requirements?

The exercises was valuable, but did not yield concrete enough results that can be used for a legal framework at this point in time. Maybe Europol can be asked to assess the viability of a more useful outcome if discussions are continued. Maybe it could be valuable if focused on a specific topic, like what data falls within the scope of determining a user's 'civil identity'.

Question: Do Member States consider there is merit in devising a targeted retention system by developing criteria to limit the means of communication or the number or type of electronic communications service providers subject to retention obligations (e.g. based on size, geographical coverage, number of subscribers, cross-border presence)?

This seems to be irrelevant for the legal scope of a potential retention obligation and more of a practical factor to consider. The preliminary view is that it should not be within the main focus of the further exploration, and potential creation, of an EU framework.

Question: Can Member States share their views of what serious threats to public security entails?

This is not exactly defined within the Dutch law and it is very unlikely that MS will share a common view on this definition and its defining elements. A parallel can be drawn with serious crime, which is another term within many EU legal frameworks that is not universally defined.

<u>Approach 3(c): expedited retention (quick-freeze) of traffic and location data for serious crime and the safeguarding of national security</u>
Questions: Given that a "quick freeze" provision can apply only if there is metadata available to "freeze", can Member States share any experience relating to the normal period of availability of metadata, absent a general retention obligation? Can Member States point to any ideas stemming from that experience that may be helpful in this context?

The Netherlands has had no legal data retention obligation since 2015. Providers are still able to produce some metadata in response to lawful requests by LEA if they have retained it for (legitimate) business purposes. In our experience though, what is retained by providers, and for how long, differs greatly – for example between ISP's and telecom provides - and changes constantly. This is thus not a reliable basis for criminal investigation or a quick freeze mechanism. Furthermore a quick freeze is less useful for investigating past crimes, because the relevant historical information, if not prior retained for legitimate business purposes by the provider, cannot be retained ad-hoc.

Can Member States share any experience relating to the use of expedited retention in their current legislation? Which options do Member States see for operationalising this mechanism to meet its objective to support investigations into serious crime and protection of national security?

We have no experience with this instrument.

Approach 3(d): generalised retention of IP addresses assigned to the source of an Internet connection for serious crime and serious threats to public security?
Questions: Do Member States see the benefits of this approach? Do they see any drawbacks in this approach e.g. that the IP address of the destination of a communication is not retained? Is there a lawful way to overcome this limitation?
Question: Are there other technical identifiers that could, in line with the jurisprudence, be captured in such legislation for example time stamps and source-port numbers to allow for identification of individuals where IP addresses are shared across multiple users, as may be the case e.g. in mobile communications?

This should be included in a broader approach containing more than only a retention scheme for IP-addresses. The retention of source IP-addresses is necessary to be able to determine the civil identity of an internet user. The biggest problem facing the effective identification is the widespread use of carrier-grade Network Address Translation technology (NAT), where several hundreds or even thousands of users use a single public IP-address. This makes it virtually impossible for LEA to identify the user of interest to the investigation. The Netherlands is currently researching how to technically overcome this problem.

Question: What cybercrimes are not currently covered by the notion of 'serious crime' in Member States' legislation?

Most cybercrimes are considered serious crimes within the Dutch criminal code. Only the following cybercrimes are not 'serious crimes'. Regretfully there is no formal English translation of these provisions available at the time of writing.

- Art. 139e Sr: Hebben en gebruiken van door wederrechtelijk afluisteren, aftappen c.q. opnemen verkregen gegevens.
- Art. 161septies Sr: Culpose vernieling van enig geautomatiseerd werk of werk voor telecommunicatie.
- Art. 350b Sr: Aantasting/manipulatie computergegevens (het culpose misdrijf).

Approach 3(e): generalised retention of civil identity data to fight crime and public security threats in general?

Questions: Is retention of 'civil identity data' effective to fight crimes? What specific elements should be included in this data category?

The Netherlands has established that this is most likely the minimum retention obligation scheme possible within the current case law of the CJEU. The investigation and potential framework by the

EC (together with MS) should thus focus on elements that can be added to the data retained for establishing the civil identity of a user.
The retention of the civil identity is a useful instrument for criminal investigations, but it is just a basic tool, amongst many others, needed to fight crime and not nearly as effective as a broader retention scheme.