Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford
douwe@korff.co.uk

KEY POINTS *RE* THE CYBERCRIME CONVENTION COMMITTEE (T-CY) REPORT:

Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY

Final report of the T-CY Cloud Evidence Group

(T-CY (2016)5, 16 September 2016)

I. The underlying problems

1. To some extent the Cybercrime Convention itself, but more specifically the authors of this report and draft recommendations, assume that the law enforcement authorities covered by the Convention and the recommendations will always act properly, in support of legitimate aims in a democratic society. Indeed, the main presumption underlying the report and the recommendations is that State-Parties to the Cybercrime Convention all, always, and in all respects, fully respect the rule of law and fully protect and ensure fundamental rights not just in relation to privacy and data protection and fairness in criminal proceedings (including criminal investigations), but also in terms of substantive law, e.g., that they do not impose undue restrictions on freedom of expression, for instance in relation to criticism of the state or the head of state, religion/blasphemy, incitement to secession, denial of the holocaust or calling another holocaust holocaust, sexual issues, intellectual property, etc.. It is only if one accepts that assumption that one can see no problems with the extra-territorial exercise of the powers covered, i.e., of the powers to directly seize evidence that is physically held in another jurisdiction.[1]

   Given that states such as Azerbadjan and Turkey are parties to the Convention (and Russia and other Council of Europe (CoE) States could join any time without a possibility of opposition; and the Convention is also open to non-CoE states), that presumption is **totally unjustified**. Does the Council of Europe really want to extend the powers of such states to collect evidence on political opponents, journalists, bloggers, etc., from databases in, say, Germany or France – without the say-so, or even the knowledge, of the governments of such target countries?

1Note that the Cybercrime Convention requires all state parties to apply their criminal procedure powers, not just to the typical (though ill-defined) "cyber crimes" listed in Chapter II, section 1, of the Convention, but to all "criminal offences [read: all acts that the state-party in question considers to be criminal] committed by means of a computer system" (Art. 14(2)(b)).

I have addressed these issues in a little detail in the *Issue Paper* I wrote for the Council of Europe Commissioner for Human Rights on The Rule of Law on the Internet and in the wider digital world, section 5.4, *Cybercrime*. Without repeating the details, I should recall that there I criticized:

- the absence of a general human rights clause from the Cybercrime Convention: the clause that refers to human rights only requires compliance with human rights law in relation to procedural matters; nor is it a condition for joining the Cybercrime Convention that the state in question is a party to the ECHR (or, in respect of non-CoE states, the ICCPR) or the Data Protection Convention. As I put it in the *Issue Paper*:

> The result is an obligation on states to criminalise certain activities, that is not counterbalanced by strong obligations and safeguards to ensure respect of human rights instruments in actually applying the criminal law to those activities. (p. 99)

the fact that the Convention clearly allows for wide divergencies in terms of substantive criminal law: even under the same provisions in the Convention, many issues and activities can be criminalised in some State Parties that do not constitute crimes in other State Parties. For instance, expressing the view that the Ottoman government's systematic extermination of 1.5 million Christian Armenians, mostly Ottoman citizens within the Ottoman Empire and its successor state, the Republic of Turkey, constituted genocide, is a crime in Turkey, while it is regarded as a perfectly lawful view elsewhere; some exceptions to restrictions on uses of copyright-protected materials in some countries (e.g., for educational purposes, or in parody) are not adopted in other countries; certain negative views of the state or heads of state or of certain religions can constitute serious criminal offences in some states but are protected in others; criminal offences relating to invasion of privacy in different countries have widely different scopes; etc.. Even in respect of the crimes defined by the Cybercrime Convention itself, state parties are expressly granted considerable flexibility in their application.[2] Consequently, as I noted, under the Convention:

2 E.g.: State parties are given the freedom to decide whether or not to adopt intent (or dishonest intent) as an element in their domestic version of the crime of "illegal access [to computer data]" (Art. 2) or in the crime of "illegal interception [of transmitted computer data]" (Art. 3); they can choose to limit the crime of "data interference" to cases that result in "serious harm" (or choose to include even trivial cases) (Art. 4); and they are given further flexibility in relation to the offences defined under the heading "misuse of devices" (Art. 6). Even in respect of the special crime defined in the Additional Protocol to the Cybercrime Convention of "Dissemination of racist and xenophobic material through computer systems" (Art. 3(1)), the protocol adds in the next two paragraphs that:
"2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply

> states can investigate and take intrusive measures in relation to activities by individuals in another state [and indeed by individuals who are nationals of and resident in that other state], even if the activities might not be criminal under the law of that other state (even if the laws in both states claim to give effect to the same provision in the convention). (p. 98, words in square brackets added)

the absence of a *ne bis in idem* (prohibition of double jeopardy) rule and of any guidance on what would be the most appropriate forum in cases in which a person might be prosecuted in several State Parties; the lack of guidance on the provisions on refusal of extradition and of mutual legal assistance (the latter of which is of course in any case rendered nugatory if states can just grab evidence from across borders without following strict requirements);

the absence of any safeguards in respect of the "spontaneous" passing on of evidence by LEAs in one country to LEAs in another state-party under Article 26; and

the fact that Article 32 of the Cybercrime Convention, which is apparently widely used in practice to circumvent MLATs, was never intended to be used in this way (see the detailed discussion in sub-section 4.5.5, under the heading "*Article 32 of the Cybercrime Convention*", pp. 102 – 106).

There is also a special problem with regards to the United States of America (USA). Although the USA is a party to the Cybercrime Convention, it refuses to recognise that it is bound by its international human rights obligations (in particular the ICCPR) in respect of anything it does outside its geographical territory in relation to people who are not US citizens or US lawful residents ("non-US-persons"). This is especially important in view of the large amount of control over data in (or passing through) cyberspace, exercised by US authorities and US corporations, including the well-known "Internet Giants", who are all fully subject to US law; and of the revelations of mass surveillance by US authorities, often acting in conjunction with such corporations, as exposed by Edward Snowden. For details, see section 3.3.2 of the above-mentioned *Issue Paper*, headed "*U.S. law*".

The T-CY Cloud Evidence Group report completely ignores the Commissioner for Human Rights' *Issue Paper* and, thus, the above issues and criticisms. This is not just a matter of any personal *amour propre* of which I might be accused – it is an indication of the general disdain with which the cybercrime LEA community treats human rights

---

paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2."

issues: they pay lip-service to it, but refuse to engage with the difficult issues in practice.

Finally, the CEG report in several places refers to EU plans as examples that should be adopted also in the context of the CoE Cybercrime Convention – but this fails to take into account that EU measures are (at least on paper) subject to the Charter of Fundamental Rights and to judicial overview (in the light of the CFR) by the CJEU. By contrast, as noted above, the Cybercrime Convention fails to ensure that measures adopted by state-parties to that convention will always conform to international human rights requirements (and the USA even formally rejects the notion that its extra-territorial actions against "non-US-persons" are subject to such requirements) and – except for state-parties to the ECHR – those measures are not subject to international judicial supervision.

I. Specific issues relating to the CEG recommendations

The report raises a large number of important and complex issues, most of them noted in an earlier paper by the steering committee, the "challenges" paper. They are set out below with brief comments.

"Cloud computing, territoriality and jurisdiction" (point 2.3): The report says in this section that "'Cloud computing' means that data is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions" (p. 7); that "It is often not obvious for criminal justice authorities in which jurisdiction the data is stored and/or which legal regime applies to [the] data" (*idem*); and that "It is often unclear whether data is stored or in transit" (p. 8). It refers to "the non-localised nature of cloud computing" (p. 9).[3]

This section also says that "Cloud service providers may take the position that governments must serve lawful orders not on them but on the owners of the data." In data protection terms, this translate as: they say they are only processors, and that the order should be served on the controllers of the processing (their clients). The report claims that:

> This often means that law enforcement must attempt to serve a series of companies or litigate whether a company actually has control of the data, all while trying to keep the target – which may be the company in control of the data – from destroying the data when it learns of the investigation. (p. 8)

On the other hand, section 3.4 makes clear, with reference to the NIS Directive, that states do not really have a problem with asserting jurisdiction, in particular not in relation to (cloud service providing) companies that have their headquarters in an EU Member State, or

3For more detail, see section 3.3 on "Loss of location".

(similar) non-EU companies that have appointed a representative in an EU Member State (who can then be served with a disclosure order).

The real problem, in my opinion, is not that data may be held in different servers in different jurisdictions, but that there are (apparently) no appropriate cross-border procedural arrangements in place to serve preservation or disclosure orders on the entities that control the cloud servers, and to have those orders enforced (subject to appropriate safeguards). In other words, this is a red herring: if the system for mutal legal assistance under Mutual Legal Assistance Treaties (MLATs) can be adequately reformed so as to (also) address the problem with "non-localised data", then the fact that data are dispersed through different servers need no longer be a real obstacle: the data may be "non-localised", but the entities controlling them are based in defined jurisdisctions, and subject to the laws of those jurisdictions. This leads to the next issue:

Mutual legal assistance (point 2.4): In this section, the report says (with reference to earlier conclusions) that:

> Mutual legal assistance remains the principal means to obtain evidence from foreign jurisdictions for use in criminal proceedings. … The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. (p.9)

It adds that "The [CoE Data Protection] Committee adopted a set of recommendations to make the process more efficient" and that "These recommendations should be implemented." (p. 9; for examples of the measures proposed, see para. 27 of the report), but then goes on to say that:

> At the same time, MLA is not always a realistic solution to access evidence in the cloud context, or it may per se be unavailable, for the reasons indicated above.

The report does not explain here, or anywhere, why full implementation of the recommendations to improve MLATs would not sufficiently resolve the problems. It appears that the authors (presumably speaking for law enforcement officials) would simply prefer to get rid of the "trouble" of having to go through the relevant formal processes, without recognizing that those "troublesome" bits of "red tape" in fact represent essential requirements of the rule of law in cross-border contexts. This is reinforced by the sections on "voluntary disclosures" of information by private sector entities to criminal justice authorities in foreign jurisdictions, noted below. As it stands, we are presented with an unexplained premise (that MLATs cannot be adequately reformed) and expected to build an entirely new, lax international legal framework around it.

"**Subscriber information"** (section 3.2): Article 18 allows for the issuing, by state parties' authorities, of "production orders" for "subscriber information"; such orders can be issued to domestic service providers, but also to foreign providers of e-communication services that offer their services in the state in question (such as the big US Internet Giants).

"Subscriber information" is expressly stipulated to not include "traffic data" or "content" (of communications), and appears to have been aimed at "the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement" (Art. 18(3)(b)). The report says that "'Subscriber information' … is, information to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person" and "also comprises data from registrars on registrants of domains" (p. 12), but Article 18 also includes "other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement" (Art. 18(3)(c)).

The concept of "traffic data" (which is expressly excluded from the concept of "subscriber data") is somewhat outdated: the Convention itself defines it as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" (Art. 1(d)); and the report says it consists of "log files that record activities of the operating system of a computer system or of other software or of communications between computers, especially source and destination of messages." (p. 12)

The report notes (with reference to an interesting questionnaire [see footnote 53]) that "Currently, practices and procedures, as well as conditions and safeguards for access to subscriber information under domestic laws vary considerably among Parties to the [Cybercrime] Convention." The authors (the CEG) are of the opinion that:

> establishing a separate regime for access to subscriber information in line with Article 18 will contribute significantly to making the MLA process regarding cybercrime and electronic evidence more efficient. A Guidance Note on Article 18 with respect to subscriber information – representing the common understanding of the Parties – is needed. It would help "facilitate greater harmonisation between the Parties on the conditions, rules and procedures for obtaining subscriber information" as recommended by the T-CY already in December 2014. It would allow using Article 18 more clearly as a legal basis for direct requests to service providers in other jurisdictions that are offering a service in the territory of a Party. (p. 23)

The report does not adequately clarify what is, and what is not, covered by the term "subscriber information". In particular, the reference in this section to "Information to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person" can potentially be read to include any data which police authorities believes is necessary to identify who has done what on the internet. This can even go beyond the assignment of dynamic IP addresses as the IP address itself is not sufficient to identify the user when CG-NAT is employed by the relevant ISP.[4] The EU Data Retention Directive, and hence most transpositions in EU MSs' laws, did not consider this limitation of shared IPv4 addresses. This has led to some police forces complaining that they cannot identify users when CG-NAT is used.

But the proposed extensive interpretation of "subscriber data", presumably in response to this issue, in fact has much broader implications. To "identify the user" in relation to CG-NATs, one would need to combine the IP address and the source port used on the public ("WAN") side of the NAT gateway. This requires retention of data about every NAT session in the NAT gateway of the ISP, which would be highly revealing about the users' intensity of using the internet. But it doesn't necessarily stop there.. In order for the IP address and source port pair to have any value, the logfiles of the websites accessed must include the source port beside the IP address, and often they do not. In the UK, this has led the Home Office to argue that full internet connection records (ICRs), that include the destination IP are "necessary" to identify the user. See Purpose 1 in this document (page 11-12) on the operational case for ICRs:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504192/Operational_Case_for_the_Retention_of_Internet_Connection_Records_-_IP_Bill_introduction.pdf

Under the Cybercrime Convention, access to "subscriber data" was made subject to a relaxed process with few real safeguards (essentially, a "self-authorising" regime for relevant authorities, without a need for judicial warrants, etc.) because it was felt that such data were not very intrusive. That presumption – and thus the relaxed regime – can only be maintained if the concept is restrictively defined and interpreted. Contrary to the implied suggestions in the report, the concept of "subscriber data" should be limited to name, address, telephone numbers and static IP addresses that are permanently assigned to the customer. This is also the definition used in Article 10(1)(e) in the

4CG-NAT stands for Carrier Grade NAT, which is often used due to the shortage of IPv4 addresses.

Directive regarding the European Investigation Order in criminal matters (2014/41/EU).[5]

5With thanks to Jesper Lund for his help on this issue.

"Voluntary disclosure" [of information, including personal data] by private sector entities to criminal justice authorities in foreign jurisdictions (section 3.5): The report contains a very interesting table showing the number of requests for data made by LEAs in the state parties to the US "Giants" Apple, FB, Google, MS, Twitter and Yahoo, and the number of "voluntary" disclosures made by these companies in response (see pp. 24 – 25). It is not clear whether the requests and responses each covered data on just one individual or account, or whether there were also single requests and disclosures relating to several individuals and accounts. Still, the figures are very interesting. The overall response rate was 60%, but there are wide variations. The companies did not provide any data in response to any of the five requests from Azerbadjan, for instance, and only complied with 17%, 25%, 26%, 28% and 31% of requests from, respectively, Cyprus, Bulgaria, Ukraine, Slovakia and Bosnia-Herzegovina. Even with regard to requests from generally more "successful" countries such as the USA itself (78% of requests resulting in voluntary disclosure), Canada (76%), Belgium (73%) or the UK (70%), it is notable that very significant numbers of requests were declined: around a quarter in these cases. The figures for some countries stand out, such as:

Turkey	16,760 requests	11,418 granted	68%
France	27,213 requests	14,746 granted	54%
Germany	29,092 requests	15,469 granted	53%

The reasons for the "success"/"failure" rates are not given. In the case of Azerbadjan, it may have to do with its bad human rights record – but in that case, it is notable that Turkey was much more "successful" in obtaining information, much more so (in percentage terms) than France and Germany.

The report notes that while US providers can disclose subscriber information with few constraints (because such data are given minimal protection under US privacy law, and virtually none if related to "non-US-persons"), the situation is different in Europe:

> While US providers are able to disclose subscriber and traffic data directly and voluntarily to foreign law enforcement authorities upon request under US law (Electronic Communications Privacy Act) this is not the case for European providers. It would seem that this often due to domestic legislation (including on data retention and e-privacy) stipulating that the data must be disclosed only to the national judicial authorities in accordance with a formal procedure [such as, in relation to foreign requests, MLATs].
>
> **The consequence is a one-way flow of data from US service providers to the law enforcement authorities of Parties in Europe and other regions, while service**

> **providers in Europe or other Parties do not disclose data directly and voluntarily to the authorities in the US or other Parties.**
>
> Increasingly, US service providers are represented within the European Union – for example through subsidiaries in Ireland – and are thus subject to European Union law, including data protection regulations. This may restrict possibilities for direct and voluntary transborder cooperation in the future.
>
> (p. 26, footnote references omitted, emphasis in bold added)

The report adds, a little later:

> European and international data protection instruments cover transborder data transfers either from one private sector entity to another private sector entity or from one competent criminal justice authority to another criminal justice authority.
>
> The "asymmetric" transfer of data from a law enforcement authority of one jurisdiction to a private sector entity in another jurisdiction in another State – for example, sending an IP address to ask for the related subscriber information – is permitted under specific conditions.
>
> **However, for the "asymmetric" voluntary disclosure of data – such as subscriber information – from a private sector service provider to a law enforcement authority in another State, clear rules permitting such transfers do not seem to be available.**
>
> Providers need to assess themselves whether the condition of lawfulness is met, whether it is in the public interest or whether it is in the legitimate interest of the provider as the data controller to disclose data. Providers may run the risk of being held liable. **A clearer framework for private to public transborder disclosure of data would be required, including conditions and safeguards.** This would help service providers avoid situations of conflicting legal obligations.
>
> (p. 27, emphases in bold added)

It also notes the anomaly that "within the European Union, a distinction is made between Electronic Communication Service providers (which are currently subject to the confidentiality requirements of the E-Privacy Directive), and Internet Society Service providers" (which are not subject to this requirement – something EDRi and others want to mend) (top of p. 27), and that "conditions for access to such data vary between the Parties": "In some, police officers and in others prosecutors can request the production of subscriber information while in some others court orders are required. In the latter case, service providers may not respond to a request from a police or prosecution authority." (p. 28)

See also the other bullet-points on pp. 25 – 29, including this one:

> Lawful requests versus voluntary cooperation:
>
> A lawful order by a police, prosecutor or judge served on a physical or legal person is binding and can be enforced on the territory of the authority.
>
> However, under the current practice of direct transborder cooperation, US service providers consider their cooperation as "voluntary". At the same time, they frequently request to be sent an order valid in the requesting country even though it is not valid in the US.
>
> The current practice appears to combine a lawful, coercive request with voluntary cooperation.
>
> US service providers seem to prefer to keep this practice.
>
> (last bullet-point on p. 28)

The CEG comments on this as follows:

> From a law enforcement perspective [the above situation] appears to be problematic as service providers determine whether or not to cooperate, evaluate the legality of the request, or check dual criminality and other conditions. This applies not only to requests for data received from police, but also prosecutors and courts; and in the end the requests are not enforceable. The fact that service providers have so much discretion is problematic from a rule of law perspective. (top of p. 29)

The report notes similar divergencies in relation to **emergency procedures**, i.e., as concerns legal rules on the exceptional disclosure of information by private-sector service providers to LEAs of state parties to the Cybercrime Convention (see section 3.6). Suffice it to note here that most (20) of the 33 state parties reviewed by the CEG "do not have legislation permitting disclosure of data by service providers to domestic criminal justice authorities in emergency situations without judicial authorisation"; that LEAs in seven of the 33 "can obtain all types of data including content while five can only obtain non-content data and one State only subscriber information without judicial authorisation"; that "Only six out of 33 States (18%) have procedures in place to disclose data to foreign authorities in an expedited manner; and that "With the exception of two States (Japan and the USA), no other State has legislation permitting a service provider in its territory to disclose data to foreign law enforcement in emergency situations without mutual legal assistance." (p. 30)

However, once again, the US companies act on their own authority in this respect too:

> Major US-based service providers have established procedures for the disclosure of data in emergency situations to domestic and foreign authorities. This may cover serious threats to the life/safety of individuals, the security of a State, commit substantial damage to critical infrastructure (Apple), imminent harm to a child or risk of death or serious physical injury to any person (Facebook), necessity to prevent death or serious physical harm to a person (Google, Microsoft, Twitter, Yahoo!). **The disclosure is at the discretion of the service provider.** They may also notify the customer either immediately or within 90 days. (p. 30, emphasis in bold added)

This contrasts with European and other providers which "do not seem to have emergency procedures in place and do not seem to cooperate directly with foreign authorities in emergency situations." (*idem*).

We can for once (somewhat) agree with the CEG that the current situation, in which (mainly US) companies determine what data to provide to which country's LEAs in which circumstances, is "problematic from a rule of law perspective". Actually, it is totally incompatible with the rule of law. Such disclosures, since they inherently constitute interferences with the rights of the individuals concerned (in particular their privacy/data protection rights) should, under fundamental European and international standards, be allowed only if they are based on (state-issued) legal rules of adequate precision and clarity to be "foreseeable" in their application; and those rules, and the way they are applied in practice, must be demonstrably "necessary" and "proportionate" to serve the legitimate aims in question (i.e., to assist in legitimate criminal investigations or to fend off an immediate threat to life or limb or public security).

It may be that, as suggested by the CEG and the CoE Committee, all of this will need to be addressed in a new protocol to the Cybercrime Convention. However, if that is pursued, the aim should not simply be, as the report seems to suggest (if perhaps somewhat *sotto voce*), to adopt the *laissez-faire* approach of the USA to "subscriber data", or to adopt rules that would simply require service providers to hand over such data to any LEA of any state-party to the Cybercrime Convention that can produce a legal order that is valid under that state-party's law. Nor should service providers be simply authorized "to respond directly to foreign requests in emergency situations as is already the case in the USA and – to some extent – Japan."

Rather, in my opinion, the emphasis should remain on improving MLATs (including implementing various proposals for common templates and language and the use of [secure] email systems, and more staffing etc.). Only if those improvements were to be conclusively shown to be

insufficient, should the idea of a new additional protocol be pursued. The onus is surely on the LEAs (and the CEG and the T-CY Committee) to provide evidence as to why MLATs cannot be adequately improved to serve the (legitimate) needs of LEAs.

Any new proposals on MLATs should clearly reinforce (or to the extent that they are not stated, introduce) the powers of state-parties to the Cybercrime Convention to refuse to comply with requests for such assistance if they fear that this could lead to human rights violations by the requesting state. States should have a duty to refuse to cooperate with MLATs if there is clear *prima facie* evidence that compliance with the request will lead to such violations.

If improved new, speedy MLATs can be made to work, the very notion that it is up to service providers to decide whether to provide information, or not, or to whom, and to whom not, should be abandoned: those disclosures should be brought under the rule of law.

IF a new protocol were to be pursued to provide a legal basis for direct requests by LEAs of state-parties to private-sector providers in other state-parties, and for mandatory compliance with such foreign orders, then there must be **extremely strong safeguards** to ensure that both subscriber data (as defined in a very limited way: see above) and other data should only be disclosed where this is fully justified, and never if this could/would be likely to result in (serious) human rights violations. Data should never be disclosed to LEAs of countries (such as the USA) that maintain that they are not bound by international human rights law in respect of the further use of the data.

International cooperation in the field of criminal justice should be based on mandatory full respect for international human rights law; countries that do not respect this should not be freely assisted in their law enforcement activities.

DK/November 2016