Practitioner's Corner

The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?

*Vanessa Franssen**

I. Introduction: Setting the 'Crime' Scene

New information and communications technologies (ICTs) facilitate our daily life in many ways. We can quickly send messages (whether by using 'traditional' email or text messages, instant messaging services such as Telegram or WhatsApp, or social media services like Facebook and Twitter) at any point of the day (and night) to anyone, no matter where we are. They allow us to exchange information extremely quickly (eg Dropbox, WeTransfer), find our way wherever we are and get updated on how bad traffic is (eg GPS or community-based navigation apps such as Waze).

Yet, the foregoing features also make ICTs highly attractive for criminal purposes. They enable criminals to commit offences from a distance, potentially targeting a large number of victims and causing tremendous harm, in great anonymity and without leaving traces. Or rather, the traces they leave are volatile and often processed by technologies companies.

Getting access to that data has become a prime concern for law enforcement authorities (ie police and judicial authorities), especially in regions like Europe and North America where people are highly connected and thus an 'easy' target of offences committed by means of ICTs, which one can refer to as cybercrime in a broad meaning. Yet, obtaining the data by the authorities is not easy, for several reasons: for instance, if the technology company is headquartered in another country, it may not be allowed to collaborate directly with foreign law enforcement authorities, it may have no access to the data requested due to the way in which its products or services are designed (eg encrypted security settings, peer-to-peer communication), it may not be allowed to keep the data due to data protection legislation, or it simply does not know where the data is stored due its specific data infrastructure.

Another related, important question for law enforcement authorities is to what extent they too can exploit ICTs in order to fight cybercriminals adequately, with the same tools. For instance, can they freely search the internet and use that information before a court of law? Can they register on internet platforms or participate in chat rooms using a fake identity when this is necessary to investigate criminal offences? Can they infiltrate a computer system to see if it contains any useful information about the offence (eg child pornographic material)? When they seize a suspect's smartphone, can they access all the data stored on the device? Can they 'hack' the smartphone's password if need be? Can they search websites visited by the owner of the device, even if they are password-protected?

These issues may at first sight seem quite technical and far-fetched, but they are daily matters of concern for law enforcement authorities in most Western countries, and since a couple of years also high on the EU agenda.[1] Often, law enforcement authorities are confronted with out-dated legislation which was created for the pre-social media era, perhaps even the pre-internet or pre-cell phone era. As a result, law

DOI: 10.21552/edpl/2017/4/18

* Vanessa Franssen, Associate Professor of Criminal Law and Criminal Procedure at the University of Liège, Senior Affiliated Researcher at the Institute of Criminal Law of the KU Leuven, and Of Counsel at Linklaters LLP, Dispute Resolution, Brussels. For correspondence: <vanessa.franssen@uliege.be>.
This publication is part of a research project supported by the Fonds de la Recherche Scientifique – FNRS under Grant No CDR J.0293.17.

1 Council of the European Union, *Conclusions on improving criminal justice in cyberspace*, Doc No ST 10007/16 INIT 9 June 2016; European Commission, *Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, Doc No 15072/16 2 December 2016; European Commission, *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward* (Non-paper, 22 May 2017) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf> all URLs in this report accessed 27 November 2017.

enforcement authorities try to 'make things work', taking benefit of the gray zones created by unadjusted rules of criminal procedure. However, this pragmatic approach raises important questions regarding the protection of fundamental rights.

In an ambitious attempt to tackle all the above issues, the Belgian legislator adopted a new legislative framework on 25 December 2016, the Act amending the Code of Criminal Procedure and the Criminal Code, with a view to improve the undercover investigatory measures and certain investigatory measures regarding the internet, electronic communications and telecommunications, and creating a voiceprint database (Internet Investigatory Powers Act).[2] This new law, which entered into force on 27 January 2017, contains a mix of provisions implementing some parts of the Council of Europe Cybercrime Convention of 2001 (Cybercrime Convention)[3], codifying the case law of the Supreme Court (*Cour de cassation*; eg on the seizure and search of smartphones without a court warrant), clarifying and modernising existing investigatory powers (eg the powers to search computer systems and to intercept content data), but also introducing new investigatory tools enabling police and judicial authorities to fight and investigate cybercrime more adequately (eg internet infiltration and covert observation of computer systems). In addition, it also provides a legal basis for the creation of a voiceprint database.

While the Internet Investigatory Powers Act obviously applies to Belgian police and judicial authorities only, it nevertheless contains a number of elements which are highly interesting for a European readership. In the subsequent overview, we will therefore present some highlights of the new law,[4] in particular the expedited preservation of computer data and the cooperation duties of service providers as these rules have certain extraterritorial effects and limit the need for mutual legal assistance. What is more, they may be a source of inspiration for other national legislators and potentially also the European Commission, as it is currently preparing a proposal for a Directive that aims at improving cross-border access to electronic evidence in criminal matters.[5]

II. Expedited Preservation of Computer Data

As indicated in the introduction, one of the objectives of the Internet Investigatory Powers Act is to further implement the Cybercrime Convention. Whereas Belgium was among the first countries to sign the Cybercrime Convention in 2001, it did not ratify the Convention until 2012. Moreover, despite that ratification, some parts of the Convention had still not been implemented. Most notably, the Belgian legal framework did not foresee the possibility to order the expeditious preservation of computer data.[6] This measure consists in preserving data that are particularly vulnerable to loss or modification for the purpose of a specific criminal investigation, pending subsequent disclosure of the data pursuant to other legal powers, such as a production order or a search and seizure.

Therefore, the Internet Investigatory Powers Act introduces two new provisions in the Belgian Code of Criminal Procedure (CCP): Articles 39*ter* and 39*quater*. The former applies to purely national situations (cf Articles 16 and 17 Cybercrime Convention), while the latter applies to cross-border situations (cf Articles 29 and 30 Cybercrime Convention), encompassing both requests issued by a Belgian com-

2 Loi du 25 décembre 2016 portant modifications diverses au Code d'instruction criminelle et au Code penal, en vue d'améliorer les methodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales *Moniteur belge* 17 January 2017 <http://bit.ly/2ADugIO>.

3 Council of Europe, Convention on Cybercrime (ETS 185) (23 November 2001) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.

4 For a more comprehensive and detailed account of the new Belgian law, we refer to other publications: Vanessa Franssen and Stanislaw Tosza, 'Vers plus de droits pour le justiciable sur internet? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information' ' in: Vanessa Franssen and Adrien Masset (eds), *Les droits du justiciable face à la justice pénale* (vol 171, Commission Universitaire-Palais, Anthemis 2017) 205-249; Vanessa Franssen and Olivier Leroux 'Recherche policière et judiciaire sur internet: analyse critique du nouveau cadre législatif belge' in: Vanessa Franssen and Daniel Flore (eds), *Le droit pénal et la procédure pénale face aux défis de la société numérique. Perspectives belges, françaises et européennes* (Larcier, forthcoming 2018); Christian De Valkeneer 'L'information et l'instruction', in: *La loi pot-pourri II: un an après* (Larcier 2017) (91) 98-130; Charlotte Conings and Sofie Royer, 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' (2017) 12(4) Nullum Crimen 311-338.

5 See in this respect, European Commission, *Improving cross-border access to electronic evidence in criminal matters - Inception Impact Assessment* (3 August 2017) <https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en#inception-impact-assessment>; European Commission, *Public consultation on improving cross-border access to electronic evidence in criminal matters* (4 August-27 October 2017) <https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en>.

6 For a more detailed analysis, see Franssen and Tosza (n 4) 224-234.

petent authority (Article 39*quater*, §1 CCP) and requests issued by a foreign competent authority (Article 39*quater*, §2 CCP). While these new provisions were presented in Parliament as a mere implementation of the Cybercrime Convention,[7] a closer look reveals the Belgian legal framework nevertheless diverges from the Convention in some respects.

1. Material Scope of Application

For a start, the material scope of application of the expedited preservation order under Belgian law is definitely wider, for two reasons.

First, unlike Article 16 Cybercrime Convention, providing for the possibility 'to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system,' Article 39*ter* CCP authorises any officer of the judicial police to order the retention of data that is *stored, processed or transmitted* by means of a computer system.[8] The wording of Article 39*ter* CCP clearly opens the door to data *retention* (in French: *conservation*), even if only for the purpose of a specific criminal investigation. This choice is peculiar because it obviously exceeds the power provided for by the Cybercrime Convention. Indeed, the Explanatory Report to the Cybercrime Convention explicitly states that the expedited preservation order laid down in Articles 16 and 17

> only refer[s] to data *preservation*, and not data *retention*' and that these articles 'do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities. (...) The articles, therefore, provide only for the power to require *preservation of existing stored data*, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings.[9]

While the discrepancy with the Convention is crystal-clear, the parliamentary documents give no explanation for the choice of the Belgian legislator. Yet, in times where the future of general data retention provisions under national law is highly uncertain,[10] the Belgian option may prove to be extremely valuable for law enforcement.

Second, the Belgian expedited preservation order is not limited to traffic data, and therefore goes beyond the minimum threshold set by the Cybercrime Convention. Based on Article 39*ter* CCP, officers of the judicial police can indeed order the preservation of other data, including content data, provided of course that there are grounds to believe that the data concerned is particularly vulnerable to loss or modification.

It should be noted that the above does not only hold true for national preservation orders, but also for transnational requests requiring mutual assistance. This may create some frictions. Indeed, in accordance with Article 39*quater*, § 1 CCP, a Belgian public prosecutor could request the competent authority of another state to preserve data that are not (yet) stored, but simple processed or transmitted in this state. However, if this state has limited the possibility of expedited preservation to stored data, as foreseen by the Cybercrime Convention, it seems likely that its competent authorities will reject the Belgian request.

2. Duty of Confidentiality

Furthermore, in conformity with the Cybercrime Convention, the persons ordered to preserve the data are obliged to preserve the integrity of the data

---

7 Explanatory Note to the Initial Legislative Proposal, Parl Doc, House of Representatives, session 2015-2016, Doc No 54-1966/01, 9 and 25-26.

8 French official version of art 39*ter* CCP: '(…) tout officier de police judiciaire peut, s'il existe des raisons de croire que des données stockées, traitées ou transmises au moyen d'un système informatique sont particulièrement susceptibles de perte ou de modification, ordonner, par une décision écrite et motivée, à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle.' [English translation: '(…) when there are reasons to believe that data stored, processed or transmitted by a computer system is particularly vulnerable to loss or modification, any officer of the judicial police can order, by a written decision giving reasons, one or more natural or legal persons to retain the data that is in their possession or under their control.']

9 See Explanatory Report to the Cybercrime Convention, para 152 (emphasis added).

10 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v T. Watson e.a.* [2016] ECLI:EU:C 2016:970. For an analysis of this case see Orla Lynskey, 'Tele2 Sverige AB and Watson et al.: Continuity and Radical Change' (*European Law Blog*, 12 January 2017) <http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> and Will R Mbioh, 'Post-och Telestyrelsen and Watson and the Investigatory Powers Act 2016' (2017) 3(2) EDPL 273-282. For an analysis of the impact of the case on the current Belgian rules on data retention, see Fanny Coudert and Frank Verbruggen, 'La conservation des données de communication électroniques en Belgique: un juste équilibre?' in Franssen and Flore (n 4).

and to keep the order confidential. A breach of either duty constitutes a criminal offence. However, it should be noted that the latter duty of confidentiality explicitly extends to all persons who, in their official capacity, *are informed of the order or help execute it*.[11] What is more, national law does not clearly indicate how long these persons are bound by the duty of confidentiality:[12] on the one hand, the preservation order can be made for a period of 90 days (though with an unlimited possibility of renewal); on the other hand, the violation of the confidentiality obligation is punished like any other violation of the professional secrecy (Article 458 Belgian Criminal Code),[13] which potentially covers the entire pretrial stage. Foreign service providers cooperating with Belgian authorities may thus not be able to inform their users concerned by the measure for a long period of time.

3. Expedited Disclosure of Traffic Data

To some extent, the Belgian legal provisions also seem to be less complete than the Cybercrime Convention. Indeed, as far as the national preservation order is concerned, they do not explicitly allow for 'the expeditious disclosure (...) of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted,' as provided by Article 17(1)b Cybercrime Convention. Nevertheless, the disclosure of such information can still be ordered on the basis of the existing duties to cooperate with law enforcement, in particular Article 46*bis* (production order relating to subscriber or identification data) and Article 88*bis* CCP (production order relating to traffic and localisation data).[14]

By contrast, with respect to transnational requests, the possibility of an expedited divulgation of traffic data is explicitly foreseen by Article 39*quater*, §2, paragraph 7 CCP. In particular, this should enable the foreign authorities to identify the service provider and the path through which the communication was transmitted if Belgium was just a transit country or if there was another state involved in the transmission of the communication (cf Article 30(1) Cybercrime Convention). The Belgian competent public prosecutor or investigating judge will disclose this data as soon as possible ('*dans les meilleurs délais*').

4. Limited Scope of Mutual Legal Assistance Due to Direct Cooperation with Foreign Service Providers

When the data that is vulnerable to loss or modification is located on the territory of another state, Belgian authorities are, in principle, required to send a request for expedited preservation to the competent authorities of that other state (Article 39*quater*, §1 CCP). For such mutual legal assistance requests, the intervention of a judicial authority is required and therefore the competent Belgian authority is not the police, but the public prosecutor, acting through the police service designated by Royal Decree.

However, it is noteworthy to highlight an important exception to this principle: whenever Belgian authorities can directly cooperate with foreign operators of electronic communications networks and providers of electronic communications services, there is no need to rely on mutual legal assistance (Article 39*quater*, §1 CCP).[15] Considering that all operators and service providers offering services in the Belgian territory are required to cooperate with the Belgian police and judicial authorities, as will be explained in Section III, the situations in which Belgian authorities will have to resort to a mutual legal assis-

11 French official version of art 39*ter*, §3 CCP: 'Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours est tenue de garder le secret.' [English translation: 'Any person who, in his official capacity, is informed of the order or helps execute it is bound to keep the measure secret.'] By contrast, art 16(3) Cybercrime Convention merely refers to 'the custodian or other person who is to preserve the computer data.'

12 It may be noted that art 16(3) Cybercrime Convention merely refers to national law: 'Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures *for the period of time provided for by its domestic law*.' (emphasis added)

13 For a general analysis of the professional secrecy under Belgian law, see eg Adrien Masset and Elodie Jacques, 'Secret professionnel' in *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, Mechelen (Wolters Kluwer, loose-leaf, updated version of December 2016) s 30, 1-27.

14 See also s III of this report.

15 French official version of art 39*quater*, §1, para 1 CCP: 'Sans préjudice des possibilités de collaboration directe avec des opérateurs de résaux de communications électroniques et des fournisseurs de services de communications électroniques étrangers (…).' [English translation: 'Without prejudice to the possibilities of direct cooperation with foreign operators of electronic communications networks and foreign providers of electronic communications services (…).']

tance request will in practice be limited to those where the operator or provider does *not* offer services in Belgium. As a fact, this comes down to a small fraction of all transnational situations...

This approach, giving preference to direct cooperation with service providers, is of course most interesting for law enforcement purposes as it avoids cumbersome and time-consuming mutual legal assistance requests. Moreover, it also seems to be the direction in which the European Commission is working.[16] Yet, a unilateral approach like the Belgian one, without a broader European or international framework, will inevitably cause conflicting legal obligations for service providers and thus raises many concerns at the international level if all countries were to proceed in this way, as the subsequent analysis will show.

III. Production Orders and Cooperation of Service Providers: 'Yahoo!'?

Another set of provisions of the Internet Investigatory Powers Act codifies controversial case law of the Belgian Supreme Court. In particular, the Act provides a legal basis for the so-called *Yahoo* case law.

1. What Preceded the New Law: The *Yahoo* and *Skype* Cases

The *Yahoo* case was, in fact, a fairly ordinary Belgian criminal case dealing with an attempt to defraud a Belgian (web) shop. The only trace left by the suspects were the Yahoo email accounts through which they had fraudulently ordered a number of products (laptops). With a view to identify the suspects, the district public prosecutor of Dendermonde ordered Yahoo! Inc. (Yahoo) to produce certain data, including the subscriber data linked to these email accounts. But since the suspects presumably used fake identities when registering for the email accounts, the public prosecutor also ordered Yahoo to give the dynamic IP addresses, the date and the time (including time zone) at which the email accounts had been created. Yahoo, however, refused to hand over the data arguing that, as an American company, it could not directly collaborate with foreign law enforcement authorities; if the Belgian public prosecutor wanted to obtain the data, he had to use the applicable mutual legal assistance procedure. Instead of going through the effort of a cumbersome mutual legal assistance procedure, the public prosecutor decided to prosecute Yahoo for refusal to cooperate – the start of very long criminal proceedings, resulting in no less than three judgments of the Belgian Supreme Court.[17]

Among the many legal questions that were raised in this landmark case were those concerning the *personal and territorial scope of application* of the cooperation duty under Article 46*bis* CCP, containing the production order for identification data. In short, the defendant Yahoo claimed that, based on a strict reading of Article 46*bis* CCP, the production order only applied to 'operators of electronic communications networks' and to 'providers of electronic communications services'; hence, a technology company like itself that only offers software allowing users of a Yahoo email account to send and receive emails anywhere in the world was not covered by the production order. What is more, the company argued that it could not be forced to cooperate with the Belgian authorities as it was not physically present in Belgium (headquarters located in the US, no office in Belgium). By contrast, according to the public prosecutor, the production order of Article 46*bis* CCP also applied to providers of webmail services such as Yahoo, and to any provider offering targeted services in the Belgian territory (ie in the local language, using a local domain name, publishing local adverts and setting up a customer complaint desk), regardless of the location of its headquarters. Indeed, the public prosecutor argued that such provider is 'virtually present' in Belgium and thus can be compelled to cooperate in a Belgian criminal investigation.

The Supreme Court ruled in favour of the public prosecutor's interpretation. In a judgment of 18 January 2011, it upheld the broad interpretation of the personal scope of application of Article 46*bis* CCP.[18]

16 European Commission, Non-paper (n 1) 3-5.

17 For a interesting analysis of the case, see Kristel De Schepper and Frank Verbruggen 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners' (2013) T Strafr 143-166; Frank Verbruggen, '"Om af te sluiten, druk op Start": zesde rechter in Belgische Yahoozaak schaart zich achter eerste' (2014) 3(2014/71) Computerrecht 129-140.

18 Cass 18 January 2017, No P.10.1347/N <https://justice.belgium.be/fr/ordre_judiciaire/cours_et_tribunaux/cour_de_cassation/jurisprudence>.

In another judgment of 1 December 2015, which put a final end to the case, it supported the prosecutor's view that any service provider offering services in Belgium can be directly forced to cooperate with Belgian police and judicial authorities, without requiring a mutual legal assistance request to the state where the service provider is headquartered.[19]

Clearly, this case law was a big victory for Belgian law enforcement authorities, as all of a sudden they obtained the possibility to compel any internet service provider, wherever in the world it is established, to cooperate and hand over data. A very tempting solution, especially in an era where almost every criminal investigation requires access to data relating to an internet service (email, app, instant messaging, social media service, etc), as explained above.

What is more, the *Yahoo* case stimulated Belgian authorities to push the boundaries even further in another exemplary case: the so-called *Skype* case. In this case, a Belgian investigating judge ordered Skype, headquartered in Luxembourg, to produce more privacy-sensitive data, in particular traffic and location data (Article 88*bis* CCP), and to intercept live communication between a couple of Armenian suspects (Article 90*quater* CCP). Like his fellow public prosecutor in the *Yahoo* case, the Belgian judge refused to apply the mutual legal assistance rules, opting instead for a direct order, without the intervention of the Luxembourg authorities. And like Yahoo, Skype refused to cooperate, invoking among other arguments that, for lack of an infrastructure in Belgium, it was not physically present on Belgian territory, that it was not allowed to hand over such private data under Luxembourg legislation and that it was even technically unable to intercept peer-to-peer communication. As a result, Skype was criminally prosecuted for failure to cooperate and convicted to a criminal fine of €30,000 by the Mechelen Criminal Court of First Instance,[20] recently confirmed on appeal by the Antwerp Court of Appeal.[21] It remains to be seen whether Skype will start a proceeding before the Supreme Court.

19 Cass 1 December 2015, No P.13.2082.N.

20 Court of First Instance Antwerp, Division Mechelen 27 October 2016, Registry No 1286, Case No 20.F1.105151-12, unpublished.

21 Court of Appeal Antwerp, 15 November 2017, Case No 2016/CO/1006, unpublished.

2. Critique of the Supreme Court's Case Law

It should be noted that the extensive interpretation by the Supreme Court of the *personal* scope of application of the cooperation duties, finds support in the definition of the term 'service providers' under Article 1 Cybercrime Convention, which includes:

> i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Still, considering the wording of Article 46*bis* CCP, one may wonder whether such an extensive interpretation by the Supreme Court was really foreseeable and thus in conformity with the principle of legality.

Moreover, the Yahoo/Skype solution raises many concerns with respect to the *extraterritorial* reach of law enforcement. If Belgian law enforcement authorities can compel any service provider which is active in its territory to cooperate, and criminally prosecute that provider if it fails to cooperate, why would other countries not do the same? Admittedly, both the *Yahoo* and the *Skype* cases were largely 'domestic cases,' ie criminal investigations relating to criminal offences committed on Belgian soil by suspects who were Belgian residents or at least presumably present in Belgium at the time of the offence. The only 'foreign' element in each case was the use of an internet service offered by a foreign service provider. Arguably, the solution of the Supreme Court would make perfect sense if it were limited to purely domestic cases. But this is not the case. As a consequence, the Yahoo/Skype approach could also be applied to offences having a very tenuous territorial nexus with Belgium.

3. Cooperation Duties under the Internet Investigatory Powers Act

Despite the obvious dangers of the unilateral Yahoo/Skype approach, the Belgian legislator decided to amend the scope of application of the existing cooperation duties of service providers, bringing them in line with the Supreme Court's *Yahoo* case law. As

a result, the cooperation duties laid down in Article 46*bis* CCP (production order for identification data), Article 88*bis* CCP (production order for traffic and location data) and Article 90*quater* CCP (obligation to provide technical assistance to enable the interception of content data) now apply to operators of electronic communications networks and any person offering, in the Belgian territory, a service which consists in the transmission of signals through electronic communications networks or which authorises its users to obtain, receive or spread information via an electronic communications network, *including* providers of electronic communications services.[22]

While the wording of these legal provisions is still not quite as general and technology-neutral as Article 1 Cybercrime Convention, the explicit objective of the legislator was to include all companies offering webmail services (eg Yahoo Mail, Hotmail, Gmail), as well as providers of social media and social networking services such as Facebook, Twitter, WhatsApp and Instagram.[23]

Interestingly, the Belgian legislator argued that the new provisions did *not* directly address the territoriality problem, in the hope to find a workable solution and consensus at EU level.[24] Nonetheless, the new legal provisions unilaterally solve a great part of the territorial problem, by obliging all services providers offering services in Belgium to cooperate with Belgian law enforcement authorities. These service providers are all required to cooperate immediately ('*en temps réel*') and to keep their cooperation confidential. The refusal to cooperate as well as the violation of the duty of confidentiality constitute criminal offences, which may result, in some cases, in imprisonment up to three years for individuals and criminal fines up to €576,000 for legal persons. Defences based on the legal or technical impossibility to cooperate are not provided for, and judging from the ongoing *Skype* case, will have a very low success rate in court. Clearly, in light of this new framework, the need for mutual legal assistance and an EU solution becomes much less pressing.

4. A Source of Inspiration for Future European Legal Instruments?

Does the Belgian approach set a good example for future evolutions at European level? As mentioned above, it is definitely a very tempting, short-term solution for national law enforcement authorities. But it may be wise to carefully consider some of its 'collateral effects'.

The immediate result of this new Belgian legal framework is that service providers operating in different countries or even worldwide (such as Google, Facebook, Twitter and Microsoft) are confronted with conflicting cooperation duties and ensuing great legal uncertainty. What is more, users of internet services are legitimately concerned about whether their personal data processed by the service provider of their choice is safe from interference from foreign governments. This explains why sever-

22 French official version of arts 46*bis*, §1, para 2 and 88*bis*, §1, para 2 CCP: 'Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:
- de l'opérateur d'un réseau de communications électroniques, et
- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques'. [English translation: 'To this end, when necessary, he can order, directly or by the intermediary of the police service designated by the King, the cooperation of :
- an operator of an electronic communications network, and
- any person who provides for or offers, on the Belgian territory, in whatever way, a service that consists in transmitting signals through electronic communications networks or in authorising users to obtain, receive or spread information through an electronic communications network. Providers of an electronic communications service are also included.']
French official version of art 90*quater*, § 2 CCP: 'Afin de permettre la mesure visée à l'article 90ter, § 1er, le juge d'instruction peut requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, le concours:
- de l'opérateur d'un réseau de communications électroniques;-
de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques'. [English translation: 'In order to enable the measure laid down in Article 90ter, §1, the investigating judge can order, directly or by the intermediary of the police service designated by the King, the cooperation of :
- an operator of an electronic communications network, and
- any person who provides for or offers, on the Belgian territory, in whatever way, a service that consists in transmitting signals through electronic communications networks or in authorising users to obtain, receive or spread information through an electronic communications network. Providers of an electronic communications service are also included.']

23 Explanatory Note to the Initial Legislative Proposal 54-1966/01 (n 8) 32-33.

24 ibid 10-11.

al global service providers are currently fighting relentless legal battles in court, not just in Europe but also in the United States (eg the so-called *Microsoft Ireland* or *Microsoft warrant* case[25]). Besides, other countries are supposedly not so happy with the violation of their sovereignty. While subscriber data are not so privacy-sensitive and thus relatively 'innocent', traffic and localisation data ('metadata') and content data are likely to create strong sovereignty conflicts in the near future if this approach is to be followed by other states.

Interestingly enough, the Cybercrime Convention Committee adopted in February 2017 a new Guidance Note on the scope of application of production orders for subscriber data, laid down in Article 18 Cybercrime Convention, which has clearly drawn inspiration from the above Yahoo case law.[26] Indeed, while Article 18(1)(b) Cybercrime Convention already applies to 'a service provider offering its services in the territory of the Party' and enables states to empower their authorities to order such service provider 'to submit subscriber information relating to such services in that service provider's possession or control', the Guidance Note clarifies the scope of application of that provision by stating that:

> Parties could apply the provision in circumstances in which the service provider offering its services in the territory of the Party is neither legally nor physically present in the territory'.[27]

Furthermore, it explains that:

> Parties could consider that a service provider is 'offering its services in the territory of the Party', when: the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services) and the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.[28]

However,

> The sole fact that a service provider makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.[29]

In other words, service providers which explicitly target users in a certain country may be required to cooperate with a production order issued by that country.

It should be emphasised that this approach so far only applies to production orders for subscriber data, *not* for other more sensitive data. That being said, the Cybercrime Convention Committee has decided to prepare a second additional Protocol to the Cybercrime Convention and, according to the Terms of Reference, the Committee will thereby consider adopting '[p]rovisions for a more effective mutual legal assistance' and '[p]rovisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests'.[30] At the same time the ambition is to create a '[c]learer framework and stronger safeguards for existing practices of transborder access to data' and provide for safeguards, 'including data protection requirements'.[31] The Council of Europe is thus clearly willing to move ahead, albeit not (yet) willing to go as far as the Belgian legislator.

What the approach of the European Commission will be, remains to be seen. It is expected the Com-

25 US 2nd Circ Court of Appeals, *Microsoft Corporation v United States of America*, 14 July 2016. The US Supreme Court granted *certiorari* on 16 October 2017 and will thus rehear the case. See for instance, Jennifer Daskal, 'Three Key Takeaways: The 2nd Circuit Ruling in the Microsoft Warrant Case' (*Just Security*, 14 July 2016) <https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case>; Orin Kerr, 'Supreme Court agrees to review Microsoft Ireland warrant case' *Washington Post* (16 October 2017) <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/16/supreme-court-agrees-to-review-microsoft-ireland-warrant-case/?utm_term=.0356e1c24331>.

26 Cybercrime Convention Committee, T-CY Guidance Note No 10, Production orders for subscriber information (art 18 Budapest Convention), adopted by the T-CY following the 16th Plenary by written procedure on 28 February 2017 <https://www.ccdcoe.org/sites/default/files/documents/COE-170228-GN10.pdf>.

27 ibid 6, point 3.2.

28 ibid 8, point 3.6.

29 ibid 8, point 3.6.

30 Cybercrime Convention Committee, Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the the Budapest Convention on Cybercrime (ETS 185), approved by the 17th Plenary of the T-CY on 8 June 2017, 3 <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b>.

31 ibid 4.

mission will publish its proposal for a Directive early 2018.[32] One can only hope that the Commission will take into account the above concerns. In our view, the envisaged legal framework should duly consider the need for adequate protection of users' fundamental rights – including also the rights to privacy and data protection – and address the problem of conflicting legal obligations of service providers, while striking a balance between the needs of law enforcement and legitimate sovereignty claims in a cloud-computing era.

IV. Conclusion

The ambition of this report was not to give a full, detailed account of the new Belgian Internet Investigatory Powers Act, but to present some interesting features from a European perspective and to put them into context with activities at EU level. To this end, we have subsequently discussed the new rules on the expedited preservation of computer data and the cooperation of service providers. As results from the analysis, the Belgian legislator clearly wanted to accommodate the needs of law enforcement, thereby sometimes going beyond the framework of the Cybercrime Convention. The new law clearly limits the need for mutual legal assistance and gives preference to direct cooperation with service providers. In doing so, this amendment to provisions in the field of criminal procedure indirectly also has a strong impact on data protection.

32 European Commission, *Improving cross-border access to electronic evidence in criminal matters - Inception Impact Assessment* (n 5).