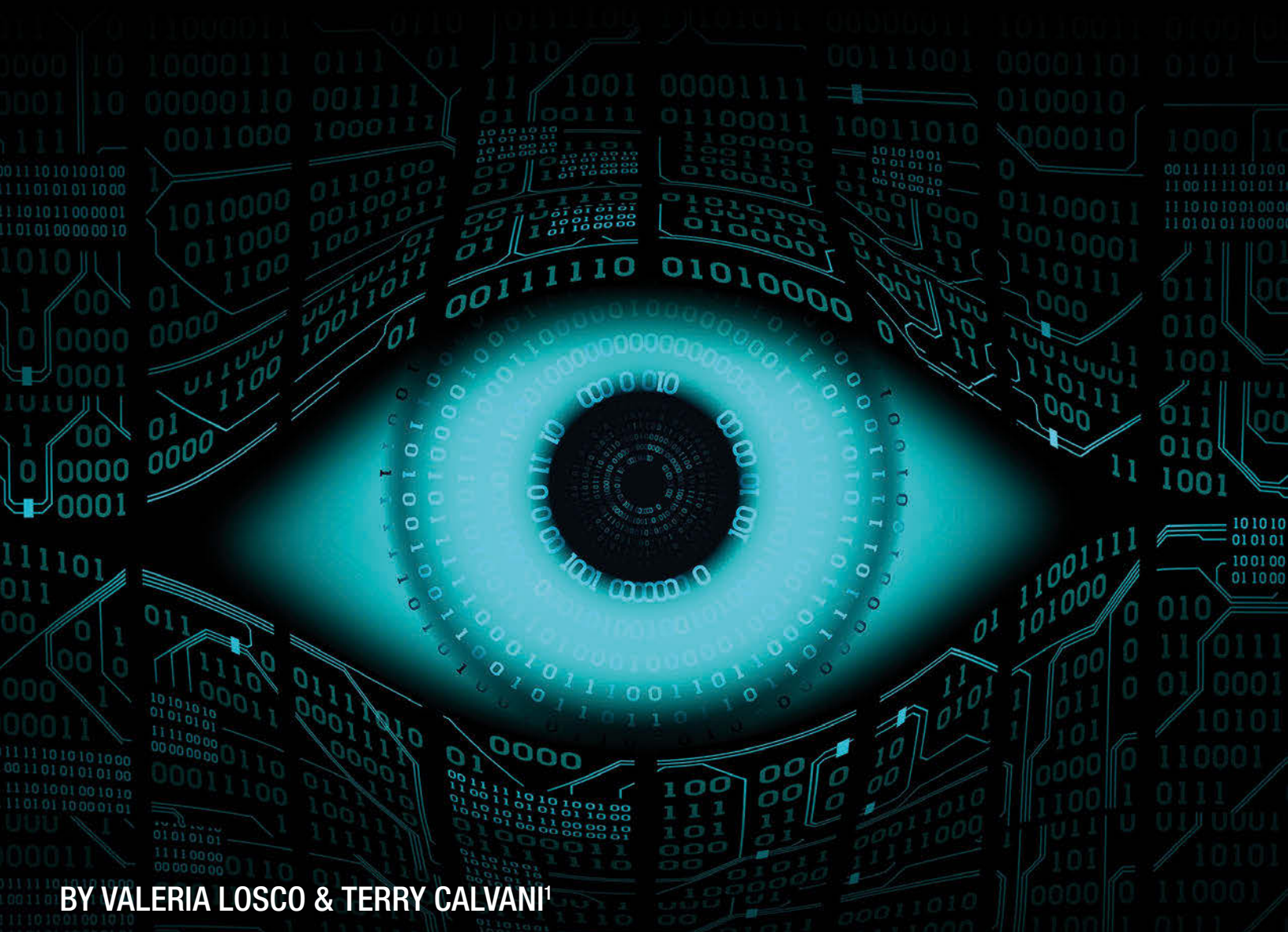
DUE PROCESS AND PRODUCTION OF DOCUMENTS STORED ABROAD: A REVIEW OF ANTITRUST DISCOVERY TOOLS AFTER *MICROSOFT IRELAND* AND THE CLOUD ACT



BY VALERIA LOSCO & TERRY CALVANI[1]

1 Valeria Losco is legal consultant at Freshfields Bruckhaus Deringer, Washington, D.C. E-mail: valeria.losco@freshfields.com. Terry Calvani is Of Counsel at Freshfields Bruckhaus Deringer, Washington, D.C. E-mail: terry.calvani@freshfields.com. The authors are grateful to Eric Mahr, Bruce McCulloch, and Mark Sansom (Freshfields) for their helpful insights and to Neil Campbell (McMillan) for his invaluable input on the sections of this article regarding Canada.

CPI ANTITRUST CHRONICLE
NOVEMBER 2018

I. INTRODUCTION

New technologies and global business practices are posing questions on how antitrust law should be applied and antitrust investigations conducted. The U.S. Federal Trade Commission ("FTC") and the European Commission ("EC") have recently launched a series of public hearings to determine whether these developments might require adjustments to competition law, enforcement priorities, and policy.[2] At the same time, the global antitrust community has been concerned about due process issues.[3] This article discusses one specific issue raised by new technologies in antitrust investigations: the production of documents stored abroad.

Until recently government agencies could only request the production of documents available in the territory where they had jurisdiction, but new technologies have challenged the concept of what is "available" in a particular territory. Daily, at work or at home, we access docum1ents and information that is not physically stored in the country where we operate. Most of the time, we do not know where the information is actually stored and we are unconcerned as this is largely irrelevant to our daily life. Yet, this matters when an antitrust agency conducts a civil or criminal investigation and requests production of documents to the parties.

Many questions arise in this context. Can an agency request only what is stored domestically, or anything parties can access from a domestic location? Does it matter if the parties can access with or without a requisite password or otherwise authorized access? If an agency can request anything that a party can access from a domestic location, is it a domestic or an extraterritorial request? What are the laws of privilege and privacy that ought to apply to information stored in one country and produced in another one?

Current law is generally silent in this regard as today's technology was not available when the legislation was enacted or when courts interpreted those laws. Over the last couple of years legislatures and courts around the globe have started to address these questions. This article will

2 Information on the "FTC Hearings on Competition and Consumer Protection in the 21st Century" is available at https://www.ftc.gov/news-events/events-calendar/2018/09/ftc-hearing-1-competition-consumer-protection-21st-century. Information on the hearings organized by Commissioner Vestager on "Shaping Competition Policy in the Era of Digitalization" is available at http://ec.europa.eu/competition/scp19/.

3 Multilateral Framework on Procedures in Competition Law Investigation and Enforcement ("MFP"), a project launched by the DOJ Assistant Attorney General for the Antitrust Division on June 1, 2018, at https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-global-antitrust-enforcement; ICN, Guiding Principles for Procedural Fairness in Competition Agency Enforcement, March 2018, at http://icn2018delhi.in/images/AEWG-Guiding-Principles-4PF.pdf; OECD, Report on Procedural Fairness and Transparency, 2012, at http://www.oecd.org/competition/mergers/50235955.pdf; ICC, Guidance on Due Process in Global Competition Law Enforcement Proceedings, June 2017, at https://iccwbo.org/publication/icc-effective-procedural-safeguards-competition-law-enforcement-proceedings/; ABA Section of Antitrust Law, International Task Force, Best Practices for Antitrust Procedure, May 22, 2015, at https://www.americanbar.org/content/dam/aba/directories/antitrust/dec15_lipsky_tritell_12_11f.authcheckdam.pdf.

review these developments and their impact on the principles of due process, with a particular focus on U.S. antitrust proceedings.[4]

II. *MICROSOFT IRELAND* AND CLOUD ACT: IMPLICATIONS FOR U.S. ANTITRUST ENFORCEMENT

The issue of the production of documents stored abroad was recently presented to the U.S. Supreme Court in *United States v. Microsoft*[5] (commonly referred as the *Microsoft Ireland* or the *Microsoft email* case), which posed the question as to whether a U.S. Department of Justice ("DOJ") search warrant issued to Microsoft as an internet service provider could require it to produce customer email data stored in a server in Dublin, Ireland.

The case stemmed from a U.S. Court of Appeals decision from July 2016,[6] which held that a DOJ search warrant on Microsoft as an internet service provider could not compel it to produce customer email data maintained in a server in Dublin. The Second Circuit found that the DOJ and other U.S. authorities do not have the power to investigate data stored outside U.S. territory as this would be an unlawful extraterritorial application of U.S. law.[7]

The U.S. government sought review of the case in the U.S. Supreme Court and, while the case was pending, on March 23, 2018, the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which requires email service providers to disclose emails within their "possession, custody, or control," even when those emails are located outside the U.S.[8] On April 17, 2018, the U.S. Supreme Court found the *Microsoft email* case moot, as the issue had been regulated by Congress. What lessons can be learned from *Microsoft Ireland* from an antitrust perspective?

Microsoft Ireland was not an antitrust case. It involved a New York-based narcotics trafficking investigation targeting an unidentified individual where the DOJ sought disclosure of emails held in a cloud-based account provided by Microsoft. The dispute arose over a search warrant issued pursuant to the Stored Communications Act ("SCA"), which authorizes search warrants for data held by electronic communications and remote computing services.[9]

4 Professor Jennifer S. Daskal, American University Washington College of Law, is an important contributor to the legal literature on the general topic of domestic and international electronic discovery and to many related issues. Anyone interested in these topics should consult her contributions to the subject. Rather than cite a long list, we point to both her SSNR authors' pages at https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1504888 or her CV at https://www.wcl.american.edu/community/faculty/cv/daskal/. We, as most anyone thinking about these issues, are indebted to her.

5 *United States v. Microsoft Corp. (Microsoft Ireland)*, No. 17-2, slip op. at 3 (Apr. 17, 2018) (per curiam) (vacating and remanding judgment).

6 *Microsoft Corp v. U.S.*, 829 F.3d 197 (2d Cir 2016).

7 In 2014, Microsoft took legal action to block a court order authorizing an investigative authority to access a Hotmail email account stored n a server in Dublin, Ireland. The U.S. government sought the emails as part of a criminal investigation, referring to the Stored Communications Act ("SCA"). The District Court held that the order against Microsoft was lawful because an authority's power to demand access to (digital) information – unlike a search warrant, which entails a physical search of premises – is not limited to the U.S., claiming that what matters is who controls the data, not where it is stored. The Court of Appeals reversed this opinion by concluding that Congress did not intend the SCA's warrant provisions to apply extraterritorially. On the Second Circuit decision of July 14, 2016, see *Data stored abroad – who controls it and where is it stored?* at https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/data-stored-abroad; B. Nevitt, *Jurisdiction, territoriality and production orders for data stored abroad,* Jan. 23, 2018 at https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=a877af7f-9b16-43bb-940e-2188c3aa7369#Footnote 1; *What powers do antitrust and competition authorities have to seize data located on foreign servers?* at http://www.nortonrosefulbright.com/knowledge/publications/143209/what-powers-do-antitrust-and-competition-authorities-have-to-seize-data-located-on-foreign-servers. For more background on the case, see *District Court Upholds Government's Ability to Seek Digital Information Stored Abroad,* Gibson Dunn, Aug. 4, 2014 at https://www.gibsondunn.com/district-court-upholds-governments-ability-to-seek-digital-information-stored-abroad/.

8 CLOUD Act, H.R. 1625, 115th Cong. div. V (2018) (enacted) (codified in scattered sections of 18 U.S.C.). The CLOUD Act, however, permits courts to exempt providers from disclosing emails of customers who are not U.S. Citizens or residents, if disclosure would risk violating the laws of certain foreign governments. 18 U.S.C. § 2703(h).

9 For other cases, this time involving Google, in which DOJ relied on the SCA to seek overseas account data, see U.S. District Court, N.D. Alabama, Northeastern Division, Sep. 1, 2017, at https://abovethelaw.com/wp-content/uploads/2017/10/In-re-Search-Warrant-Issued-to-Google-Inc._2017-10-25-11-34-33-0400.pdf; U.S. District Court for the Northern District of California, Apr. 19, 2017, at https://dlbjbjzgnk95t.cloudfront.net/0915000/915244/https-ecf-cand-uscourts-gov-doc1-035115371508.pdf; U.S. District Court for the Eastern District of Pennsylvania, Feb. 3, 2017, at https://www.justice.gov/archives/opa/blog-entry/file/937001/download.

III. U.S. ANTITRUST DISCOVERY TOOLS AND PRODUCTION OF DOCUMENTS STORED ABROAD

The SCA allows "a government entity" (which includes the DOJ Antitrust Division) to use warrants for the disclosure of electronic communications by a third party provider. Although the DOJ Antitrust Division is such a "government entity" under the SCA, to our knowledge, it has never used these warrants in antitrust investigations.

We are also not aware of any case where the U.S. DOJ Antitrust Division has used other potential avenues, such as a search warrant or a grand jury subpoena, to collect data from a third party internet provider. Similarly, the Antitrust Division does not appear to have released any specific guidance or statement in this respect. Furthermore, the sections of the Division Manual on Grand Jury Subpoena and Search Warrants have not changed regarding access to data stored abroad.

A. U.S. DOJ Grand Jury Subpoena

The Division Manual on Subpoenas Duces Tecum (section updated on April 2018) includes the following statement:

> Efforts to obtain evidence located outside the United States present special considerations. Staff should consult with the International Section to discuss possible methods of obtaining such evidence, including alternatives to subpoenas.[10]

In practice, while grand jury subpoenas require the production of all materials within the custody, possession or control of the recipient wherever located, the cover letter accompanying the subpoena always, in our experience, explicitly states that the DOJ does not demand the production of such materials when located abroad. Voluntary production of those same materials is welcome.

B. U.S. DOJ Search Warrants Executed on Premises with Access to Foreign Stored Data

Similarly to grand jury subpoenas, when search warrants are executed, terminals are used to access materials located within the U.S. but not those hosted outside the U.S.

To our knowledge, the Antitrust Division has not issued guidance on the production of electronic information hosted on a server outside the U.S. but accessible by the parties through terminals in the U.S., suggesting that the Antitrust Division intends to preserve the option of evaluating each situation on a case-by-case basis.[11]

Similarly, access to password protected information should be viewed as a fact specific question. It is common practice nowadays to have password protected electronic devices. Again, absent specific circumstances, if custodians can access password protected information stored abroad on a regular basis, it would be difficult to argue that they do not have "possession, custody, or control" over this information. The situation would be different if the same custodians could have obtained the password or restricted access, but they never sought or obtained it. In this situation it seems plausible that the Antitrust Division would take the position that these custodians did not have "possession, custody, or control" over that information.

C. Private Treble Damage Subpoenas

On the private litigation side, plaintiffs have no other public policy consideration and always demand documents located abroad if they are in the custody, possession, or control of the defendant, even if foreign law forbids their production.[12] Courts are generally often willing to order production even when foreign governments themselves have asserted that such production would violate the law if the court thinks that the threat of

10 See page III-86 of Division Manual, Fifth Edition, at https://www.justice.gov/atr/division-manual.

11 The section on search warrants of the Division Manual is silent in this respect. See page III-90, Division Manual, Fifth Edition, at https://www.justice.gov/atr/division-manual. Guidance on this issue is also not provided by the Criminal Division's Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, which was last updated in 2009. This document is available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

12 On the specific topic of discovery in U.S. antitrust litigation of European Commission materials, see T. Calvani, J. Mellott, Discovery of European Commission Materials in U.S. Civil Antirust Litigation: An Update, Concurrences N° 1-2015.

sanctions has been orchestrated by the defendant and is not real.

IV. A LOOK AT HOW THE ISSUE IS ADDRESSED IN OTHER JURISDICTIONS

A. Canada

While there is no judicial authority that addresses the power of competition authorities to seize data located on foreign servers, the Canadian Competition Act (Section 16.1. "Operation of computer system") provides that the Commissioner can obtain a court warrant authorizing the search of computer systems for "any data contained in or available to the computer system." Such data could arguably include data accessible from the Canadian computer but located on a foreign server. Thus, Canadian practice may be more permissive than that of the U.S.

Furthermore, the Canadian Commissioner of Competition can obtain a court order requiring a Canadian corporation to produce relevant records of an affiliate, even if the affiliate is outside Canada. There has been litigation challenging the constitutionality of this provision, but each time it has settled or has been abandoned. There is therefore no legal certainty regarding the application of this provision. The Canadian Commissioner of Competition considers these as domestic requests for a warrant from a Canadian court relating to physical premises in Canada.

With respect to the question on password protected information, the Canadian Competition Act (Section 16.2) states that the person in possession or in charge of the premises searched shall permit the officers executing a warrant "to use or cause to be used any computer system or part thereof on the premises to search any data contained in or available to the computer system" and to produce a copy.[13] The Commissioner's position is that one can be required to provide a password. Again, there is a possibility for constitutional challenges and we are not aware of definitive jurisprudence on this issue.

In terms of Canada's approach to legal professional privilege and data protection, there is no conclusive authority. However, we are not aware of any instances in which the Commissioner's staff has attempted to apply lower levels of privilege protection from foreign jurisdictions (e.g. Europe, which does not consider the advice of an in-house counsel to be protected by attorney-client privilege).

We also note that in some of the competition class actions (e.g. in the financial sector) we are seeing defendants and plaintiffs deal with settlements in a manner that respects privacy laws of both domestic and applicable foreign jurisdictions. However, these are uncontested court orders.

B. European Union

There is little guidance with regard to the European Commission's authority to search and seize electronic documents located on foreign servers.[14] More guidance seems to come from Member States, as is illustrated below.

Things may change should the pending proposal for an EU Regulation on European Production and Preservation Orders for electronic evidence in criminal matters be approved by the European Parliament and Council.[15] The new Regulation, which is currently available as a first draft, will focus on facilitating the process for collecting evidence abroad. Specifically, the Regulation would introduce binding European Production and Preservation Orders that would be issued or validated by a judicial authority of a Member State. These orders would be issued to seek the preservation or production of data that is stored by a service provider located in another jurisdiction, and that are necessary as evidence in criminal investigations or criminal proceedings. Both Orders could be served on providers of electronic communication services, social networks, online marketplaces, other hosting service providers, and providers of internet infrastructure such as IP address and domain name registries. Such Orders may only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State. It appears, therefore, that this Regulation would only apply to Member States with criminal competition law sanctions already in place.

13 S. 487(2.1) of the Criminal Code contains a similar provision, while S. 487.02 of the same code allows the issuing court to order a person to provide assitance.

14 See *What powers do antitrust and competition authorities have to seize data located on foreign servers?*, Norton Rose Fulbright, 2016, at http://www.nortonrosefulbright.com/knowledge/publications/143209/what-powers-do-antitrust-and-competition-authorities-have-to-seize-data-located-on-foreign-servers.

15 See proposal for a Regulation of the European Parliament and of the Council of the European Union on European Production and Preservation Orders for electronic evidence in criminal matters (April 2018), at https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

C. United Kingdom

There is no direct provision or published guidelines from the Competition Market Authority ("CMA") indicating that the CMA can search data located on a foreign server. Yet such data could be copied or taken away when it is "accessible." Indeed, according to Section 28A(2)(f) of the Competition Act of 1998 inspecting officers are entitled "to require any information which is held in a computer and is accessible from the premises and which the named officer considers relates to any matter relevant to the investigation, to be produced…"

The CMA (and the UK sector regulators with concurrent jurisdiction to enforce the Competition Act) takes the view that they are able to use their document production powers to compel the production of any documents that can be accessed from a domestic location. It does not appear to matter whether the information can be accessed with or without a requisite password or otherwise authorized access. The CMA can indeed require the undertaking concerned to provide any passwords needed to access information that it regards as within its jurisdiction to obtain. Requests to produce information on foreign servers that parties can access from a domestic location would be treated as a domestic request falling within the scope of the Competition Act's powers.

This approach seems to be confirmed by a recent UK case concerning not the CMA, but the UK Serious Fraud Office (SFO). Interestingly, on September 6 of this year, the English High Court ruled in *R (KBR Inc.) v. The SFO* on the SFO's power to compel the production of data held overseas.[16] According to this decision, the scope of the SFO's power to compel the production of data extends to:

- data of a UK company held abroad; and
- data of a non-UK company held abroad, provided there is a "sufficient connection" between that company and the UK.

The Court clarified that the "sufficient connection" test is necessarily fact-specific, and refused to limit itself to a fixed list of relevant factors. However, the Court did mention that a sufficient connection might exist where:

- A non-UK company carries on business in the UK; or
- where there is evidence that a non-UK company is actively involved in the matters being investigated by the SFO, including where the company has a UK-based employee at the time of the matters being investigated.

Merely being the parent of a UK company, or having already voluntarily assisted the SFO with its investigation, would not, in itself, constitute a sufficient connection with the UK. The SFO's power to directly order the production of data stored abroad under the circumstances clarified above is viewed by the Court as an alternative tool to the Mutual Legal Assistance Treaties ("MLAT"), which allow the SFO to request information stored abroad through foreign authorities.

A Bill of last June could make this decision less relevant, at least for documents stored electronically in countries that have reciprocal arrangements for the recognition of production orders.[17] The "Crime (Overseas Production Orders) Bill" will provide law enforcement agencies and prosecutors the option to apply for a UK court order to get stored electronic data directly from a company or person based outside the UK for the purposes of criminal investigations and the prosecution of serious crimes.

Currently, when UK agencies are seeking access to data for evidence purposes - and that data is held by providers based overseas – they must seek access to the data using MLAT, which can be slow and cumbersome. This legislation will allow law enforcement agencies and prosecutors to apply directly to service providers based in a territory with whom the UK has a relevant international agreement, by way of a UK

16 Case No: CO/4915/2017 at http://www.bailii.org/ew/cases/EWHC/Admin/2018/2368.html. See J. Kelly, *Non-UK company with non-UK data: Serious Fraud Office's information powers can still bite,* Sep. 6, 2018, at http://risk.freshfields.com/post/102f1p2/non-uk-company-with-non-uk-data-serious-fraud-offices-information-powers-can-st.

17 The text of the Bill is available at https://services.parliament.uk/bills/2017-19/crimeoverseasproductionorders.html. For a comment on this Bill, see *SFO Successfully Defends Challenge Over the Territorial Scope of Compulsory Document Requests,* Gibson Dunn, Sep. 11, 2018, at https://www.gibsondunn.com/wp-content/uploads/2018/09/sfo-successfully-defends-challenge-over-territorial-scope-of-compulsory-document-requests.pdf.

court approved order[18]. This will make the process for gaining access to this type of data faster and more reliable.

Generally, the CMA (and sector regulators) would apply the UK's law on privilege to any materials disclosed in response to a UK investigation conducted under Competition Act powers. However, the applicable guidelines (OFT404, paras 6.2 to 6.4) clarify that where material is provided to the CMA by another agency in a jurisdiction where that material was not privileged from disclosure to the foreign agency, then the CMA would be entitled to use that material regardless of the UK's privilege position in relation to it.

D. Belgium

In Belgium, a Supreme Court decision of December 2015 allowed Belgian authorities to request Yahoo! to provide subscriber data on the identity of certain individuals who had used their free Yahoo! email account to commit fraud in Belgium. The authorities' request was based on Article 46*bis* of the Belgian Code of Criminal Procedure, which states that electronic communication service providers operating in Belgium are obliged, under certain circumstances, to disclose subscriber information to the Belgian authorities for the purposes of a criminal investigation.[19]

The Belgian Supreme Court did not treat this as an extraterritorial request even where the information requested was stored outside Belgium. The Court reasoned that Yahoo! was "actively participating in the economic activity in Belgium" by using a local domain in Flemish and French (i.e. www.yahoo.be), showing advertisements directed to Belgian consumers and creating a local complaint box and helpdesk.

The same approach was followed by the more recent case involving Skype, which confirmed the legitimacy of domestic production orders on foreign companies providing a service in Belgium.[20] In this case, a court in Mechelen imposed a EUR30,000 fine on Skype for producing only metadata in the context of an investigation involving a criminal gang that used Skype to communicate. On November 15, 2017, the court of appeals of Antwerp rejected Skype's appeal and confirmed the fine.[21]

V. CONCLUSIONS

The production of documents stored abroad appears to be an area primarily handled according to local practices with little guidance from national laws or antitrust agencies. The issue is probably evolving so fast, due to new technologies, data storage, and management tools unimaginable only a few years ago, that legislators struggle to keep up. New bills are pending and courts in different parts of the world are expanding national tools and ruling on obligations of foreign companies to produce documents stored abroad in case of a sufficient connection of the company with the jurisdiction where the enforcer is located. These developments occur primarily with respect to criminal investigations and fraud cases. Additional considerations, such as the protection of privileged information and data privacy issues are making the production of documents stored abroad even more complicated. Companies in the EU or elsewhere may have to comply with rigorous data privacy regulation without being able to use it to defend against the production of information in other jurisdictions where such data is accessible through local terminals.

18 According to this Bill, "International co-operation arrangement" means "an international agreement, instrument or other arrangement which relates to the provision of mutual assistance in connection with the investigation or prosecution of offences and to which the UK is a party or in which the UK participates." If the Bill becomes law and agreements are put in place, it should become easier for government officials to obtain electronic data from abroad.

19 *Hof van Cassatie of Belgium, YAHOO! Inc.*, No. P.13.2082.N of Dec. 1, 2015. An English translation of this decision is available at http://journals.sas.ac.uk/deeslr/article/viewFile/2310/226. See Nevitt, *Jurisdiction, territoriality and production orders for data stored abroad,* Jan. 23, 2018 at https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=a877af7f-9b16-43bb-940e-2188c3aa7369#Footnote 1.

20 *Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium,* No. ME20.F1.105151-12, Oct. 27, 2016, at http://www.wolterskluwer.be/files/communities/legal-world/rechtspraak/2016/Corr.%20Mechelen%2027%20oktober%202016%20(Skype).pdf.

21 It is worth mentioning that in addition to the UK and Belgium decisions, a similar case was brought before a court in The Netherlands. The case did not lead to a decision on the merits thought. The case assessed the legality of a production order for content data served to a Dutch provider of fiscal cloud software. The requested data was stored in servers in Ireland, rented by the Dutch company from Amazon. The cloud software provider had filed a complaint against the production order to the Overijssel District Court. The Overijssel District Court explicitly acknowledged that the data requested under the production order was stored in Ireland but failed to address any issues of possible extraterritorial enforcement and declared the complaint made by the cloud software provider unfounded on other grounds. Overijssel District Court, Feb. 1, 2017, ECLI:NL:RBOVE:2017:417.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 20,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.