COMPUTER LAW & SECURITY REVIEW ■■ (2018) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law

Paul de Hert [a,b,*,†,§], *Cihan Parlar* [c,‡,§], *Juraj Sajfert* [d,¶]

[a] *Vrije Universiteit Brussel (LSTS), Belgium*
[b] *University of Tilburg (TILT), The Netherlands*
[c] *Vrije Universiteit Brussel, Belgium*
[d] *European Commission, Brussel, Belgium*

Keywords:
Cybercrime
Budapest (cybercrime) convention
Production order
Sovereignty
Extraterritoriality
Electronic evidence
Mutual legal assistance
Service providers
Enforcement jurisdiction
Criminal justice in cyberspace

A B S T R A C T

This article provides a critical analysis of the Council of Europe Cybercrime Convention Committee's Guidance Note of Production Orders, published on 1 March 2017. The article looks at the legal controversies surrounding production orders with a cross-border element. It explains the Guidance Note's background and origins, the basic provisions in the Cybercrime Convention allowing the law enforcement authorities to order and obtain certain information and discusses the requirements that follow from the relevant provisions of the Convention. This analysis is complemented by four critical remarks on the way the Guidance Note pushes the boundaries of acceptable treaty interpretation on the necessity of the Guidance Note, its position in regard to extraterritorial enforcement jurisdiction and sovereignty, its reticence towards fundamental rights and its refusal to define or clarify the important notion of "subscriber information". The article argues that unilateralism is not a solution. Instead of soft law plumbing, what is needed is an agreement between sovereign states checked by their constituencies.

* *Corresponding author.* Vrije Universiteit Brussel (LSTS), Belgium and the University of Tilburg (TILT), The Netherlands.
E-mail address: paul.de.hert@vub.ac.be (P. de Hert).
† Professor at the Vrije Universiteit Brussel (LSTS), Belgium and the University of Tilburg (TILT), The Netherlands
§ de Hert and Parlar are researchers in the DG Justice project "Criminal Justice Access to Digital Evidences in the Cloud – '**LIVE_FORensics**' (LIVE_FOR)"
‡ Doctoral Candidate and Researcher in the fields of Data Protection and Cybersecurity at Vrije Universiteit Brussel, Belgium.
¶ Official of the European Commission. The views expressed in this article are purely those of the writers and may not in any circumstances be regarded as stating an official position of the European Commission.
https://doi.org/10.1016/j.clsr.2018.01.003

Please cite this article in press as: Paul de Hert, Cihan Parlar, Juraj Sajfert, The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.01.003

1. Introduction

The criminal landscape is growing in complexity and sophistication. More and more crimes are committed online or are at least somehow facilitated by a computing device such as a mobile phone, tablet or PC. That is why electronic evidence is nowadays involved in almost all criminal investigations.[1] Since the internet usage is genuinely interlaced with some form of service provider such as telecommunications services, electronic communications services, information society services and cloud services providers, a crucial quantity of digital evidence accumulates at these intermediaries. Compelling service providers to disclose data via production orders, comprehensibly, has become a significant building block in (modern) criminal investigations.

Law Enforcement Authorities (LEAs) and their territorially restricted investigatory powers, encounter complex and yet unsolved sovereignty questions, when compelling service providers for data. This is because the respective service provider might either be established abroad, and/or is storing the data sought after outside the investigating State's territory. Using the official channel of investigation, mutual legal assistance, is regarded as being burdensome and slow,[2] in particular where the establishment of the service provider abroad or data storage abroad is the only cross-border element of the case.[3] It is therefore not surprising that (data) production orders with a cross-border dimension have been causing challenges before the courts in the US and Europe, accompanied by political debates.

Cases such as *Microsoft Ireland*[4] (2016) in the US as well as *Yahoo! Belgium*[5] (2007–2015) in Europe, underline the discrepancy surrounding the (extra-)territorial reach of investigatory measures or more general enforcement jurisdiction. The Council of the European Union, in its efforts to improve criminal justice in cyberspace, concluded, that the European Commission should "explore possibilities for a common EU approach on enforcement jurisdiction in cyberspace in situations where existing frameworks are not sufficient, e.g. [. . .] situations where relevant e-evidence moves between jurisdictions in short fractions of time [. . .]".[6] The Commission was especially requested to determine "which connecting factors can provide grounds for enforcement jurisdiction in cyberspace" and "whether, and if so which investigative measures can be used regardless of physical borders".[7]

The Council of Europe's (CoE) Budapest Cybercrime Convention (CCC) entered into force in July 2004 and was so far ratified by 43 out of 47 Members of the Council of Europe (San Marino, Ireland, Russia and Sweden have not ratified it) and USA, Canada, Israel, Chile, Costa Rica, Dominican Republic, Japan, Mauritius, Panama, Senegal, Sri Lanka, Tonga and Australia. The CCC is in fact not limited to mere matters of cybercrime but also embraces investigatory measures concerning "the collection of evidence in electronic form" of any form of offence where such electronic evidence may be relevant.[8] The CCC with its 56 Contracting States constitutes the first and most significant multilateral binding instrument to regulate cybercrime, some might even say, "the most complete international standard to date".[9] In resonance to the aforementioned concerns, the Cybercrime Convention Committee (T-CY) of CoE, representing the signatory States of the CCC, adopted in March 2017 a Guidance Note concerning the interpretation of Article 18 CCC in regards to "Production orders for subscriber information" (hereinafter *Guidance Note*).[10]

[1] Susan W. Brenner, Cybercrime: criminal threats from cyberspace, 2010, p. 37.

[2] See Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 12th Plenary (2–3 December 2014), page 123: "The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence."; similar views have also been expressed by service providers, for instance Google: Kent Walker, Digital security and due process: A new legal framework for the cloud era, The Keyword (Google Blog) (22 June 2017), accessible under https://www.blog.google/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/ (checked: 18.08.2017); for scholarship see *inter alia* Bert-Jaap Koops & Morag Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law, Tilburg Law School Research Paper No. 5/2016, (2014), page 14.

[3] For example, both the perpetrator and the victim of a crime committed in France could be French citizens and residents. The investigation will be carried out by French police and French prosecutors. However, they might have to acquire certain electronic evidence from a non-French service provider.

[4] U.S. Court of Appeals for the Second Circuit, *Microsoft v. United States*, No. 14–2985 (2d Cir. 2016), 14.07.2016; In its last attempt to challenge the decision, the Department of Justice (DOJ) in June 2017 has asked the Supreme Court to hear its appeal in the case. The Supreme Court granted the DOJ's petition to review on October 16th, 2017.

[5] Decision by the Belgian Court of Cassation (2015), see unofficial translation of the case in Digital Evidence and Electronic Signature Law Review, Volume 13 (2016), page 156–158, accessible under http://journals.sas.ac.uk/deeslr/article/view/2310 (last checked: 29.06.2017); especially addressing the early stages of the case Paul de Hert & Monika Kopcheva, International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case, Computer & Security Review 27 (2011) 291–297.

[6] Press Release, Council of the European Union, Council Conclusions on Improving Criminal Justice in Cyberspace, 2016, (hereinafter: Council Conclusions), conclusion point 10.

[7] Ibid. conclusion point 11.

[8] Article 14 (2) (c) CCC.

[9] Jonathan Clough, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation, 40(3) Monash University Law Review 698–736 (2014), at 734.

[10] Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention), revised version as adopted by the T-CY following the 16th Plenary by written procedure (28 February 2017). 01.03.2017, available at https://rm.coe.int/16806f943e (last checked: 29.06.2017).

Please cite this article in press as: Paul de Hert, Cihan Parlar, Juraj Sajfert, The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.01.003