COMPUTER LAW & SECURITY REVIEW 31 (2015) 719–735

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Transborder access and territorial sovereignty

Anna-Maria Osula *

Faculty of Law, University of Tartu, Estonia

Keywords:
Transborder access
Remote search and seizure
Territoriality principle
Jurisdiction to enforce

A B S T R A C T

The increasing sophistication of malicious cyber activities and the associated challenges with addressing these threats continue to underline the urgency of effective investigative measures for law enforcement authorities. This is especially relevant in investigations where the necessary data to be obtained are stored in a foreign jurisdiction, and access to that data may require additional legal authority. Given that traditional mutual legal assistance treaties are not entirely suitable for the volatile nature of electronic evidence, options for remotely accessing transborder data have been proposed both by nations and international organisations. Despite having been discussed by scholars and policy-makers for almost two decades, the legitimacy of such transborder access has not been readily accepted. In this context, interpretations that pertain both to the scope of jurisdiction to enforce and the principle of territorial sovereignty are particularly fragmented. This article compares the different approaches proposed in academic literature with developments in State practice and international organisations. The article concludes that transborder access can be generally seen as an extraterritorial application of jurisdiction to enforce and therefore, in order to avoid breaching the other State's sovereignty, such investigative activities should have explicit legal grounds.

1. Introduction

With a total of 3 billion users having access to the Internet by the end of 2014,[1] and the explosive expansion of devices already or soon-to-be able to connect to the Internet,[2] the large majority of current and future criminal investigations will make use of evidence either stored on or transmitted via electronic devices. While it is apparent that the legal, procedural, and technical aspects of electronic evidence are, and will increasingly be, relevant for all legal proceedings, the challenge of extraterritorial electronic evidence is particularly evident in the context of cyber crime.

Reasons for this lie within the transnational nature of cyber crime offences that more often than not involve actors, actions, or substantial effects that are wholly or in some part located at or have been carried out in another jurisdiction.[3] For example, the recent Zeus 'Gameover' botnet infected 500,000–1,000,000

* Faculty of Law, University of Tartu, Näituse 20, 50409 Tartu, Estonia.
E-mail address: annamaria.osula@gmail.com.

[1] International Telecommunication Union, 'ICT Facts and Figs. 2014' (2014) <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>.

[2] According to the UN study, 'by 2020 the number of networked devices will outnumber people by six to one'. Read more at United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (2013) xvii <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

[3] According to ibid., 'between 50 and 100 per cent of cybercrime acts encountered by the police involve a *transnational* element.' Ibid. xxv, 117–118.

http://dx.doi.org/10.1016/j.clsr.2015.08.003

computers worldwide, and its investigation included private industry experts and law enforcement counterparts in more than 10 countries.[4] The Zeus case underlines that the investigation and the subsequent prosecution of transnational cases depend on not only harmonised substantial and procedural criminal law but also on effective operational mechanisms for international cooperation.

Importantly, successful prosecution must be supported by relevant evidence, which in order to be admissible in court needs to be obtained in a way and in a format that is in accordance with legal limitations. In cases of transnational crime such as cyber crime, law enforcement often needs to locate and access evidence that may be residing in multiple jurisdictions, or the location of which may, due to the distributed nature of cyberspace (e.g. the widespread use of cloud computing), be impossible to identify at a given time.[5]

For decades, mutual legal assistance treaties (MLATs), formal multi- or bilateral-framework agreements negotiated between States, have been used to obtain evidence from another jurisdiction without challenging the signatory State's territorial sovereignty. Reportedly, approximately 70% of the means of international cooperation in cyber crime investigations are based on these mechanisms.[6] However, these traditional means for accessing extraterritorial data may not satisfy modern criminal procedures in terms of time efficiency. It may take months for the extraterritorial evidence to reach the requesting State, and such inflexibility as to the speed of MLA mechanisms renders them largely unsuitable for the volatile nature of electronic evidence.[7] In addition to the inherent slowness of MLAT procedures, there can be other difficulties related to acquiring the necessary legal grounds for accessing evidence extraterritorially. For instance, situations exist where: MLATs do not cover such topics as transborder access; there are no MLATs in place whatsoever; the other State is simply uncooperative; where accessing the data is urgent in order to avoid it being destroyed; or where it is impossible to identify the jurisdiction of the data altogether.[8]

Imagine a situation, where during a warranted search and seizure of a house, investigators locate the suspect's computer, turned on with full and open access to the suspect's data (and it is critically important to access that data as soon as possible). What are the legal limits of the activities of the law enforcement if it is clear that the data are not stored in the suspect's desktop computer but in servers located in foreign territories or if it is not possible to determine the exact location of the data? What are the different options for accessing such data, when MLAT procedures may not be best fitting for the time-critical nature of the investigation?[9]

Over time, States have developed a number of alternative measures for obtaining extraterritorially located data. Known options include formal or informal cooperation between different countries' law enforcement and establishing national 24/7 point of contact networks. In addition to these State-to-State options, additional means for accessing data can be characterised by a certain extent of 'sidestepping' the State as the determining factor for the location of the data. These methods include inquiring for the data directly from third parties such as Internet Service Providers (ISPs); accessing data publicly available; accessing data with the consent of the owner of the data or a 'lawfully authorised entity'; as well as directly accessing[10] the data regardless of its physical location.[11]

Legally, the most controversial among the numerous ways for law enforcement to secure evidence for prosecution is 'transborder access'. Within this article, the term 'transborder access' is employed as signifying unilateral access (i.e., accessing, copying, seizing)[12] to computer data stored in another jurisdiction without previously seeking specific mutual

[4] US Department of Justice, Press release, June 2, 2014, U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator, <http://www.justice.gov/opa/pr/2014/June/14-crm-584.html>.

[5] The inability of identifying the exact location of the data at any given time is known as 'loss of location'. Read more at Jan Spoenle, 'Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?' (CoE 2010) Discussion paper <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df>; see also Koops, B.-J. and Goodwin, M., 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation' (2014) 42 <http://english.wodc.nl/images/2326-volledige-tekst_tcm45-588171.pdf> on their proposal to prefer the use of term 'loss of knowledge of location'.

[6] United Nations Office on Drugs and Crime (n 2) 201.

[7] Read more at Council of Europe, 'Electronic Evidence Guide' (Data Protection and Cybercrime Division 2013) Version 1.0 11.

[8] See, e.g. New Zealand and Law Commission, *Search and Surveillance Powers* (Law Commission 2007) 226; Council of Europe, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime' (Cybercrime Convention Committee (T-CY) 2014) T - CY(2013)17rev <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf>; Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data' (2015) Vol 9 Masaryk University Journal of Law and Technology.

[9] For a comprehensive overview of this and other similar scenarios together with the results of a survey describing various State practice, see Council of Europe, 'Transborder Access and Jurisdiction: What Are the Options?' (Cybercrime Convention Committee (T-CY) 2012) <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8>.

[10] It has been reported that law enforcement may, in practice, through a number of means, directly access extraterritorial data – either with or without the knowledge of investigators. United Nations Office on Drugs and Crime (n 2) 222–223.

[11] Some of these options are described in more detail in Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Siani Pearson and George Yee (eds), *Privacy and security for cloud computing* (Springer 2013).

[12] It has also been proposed to view transborder access not as accessing extraterritorially located data but rather as 'sending and receiving messages' since this may alter the assessment of the lawfulness of the activity. Koops, B.-J. and Goodwin, M. (n 5) 50–51.