Organisation for Economic Co-operation and Development

DAF/COMP/GF/WD(2018)37

Unclassified

English - Or. English

26 November 2018

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Global Forum on Competition

INVESTIGATIVE POWERS IN PRACTICE – Breakout Session 1: Unannounced inspections in the digital age - Contribution by South Africa

- Session IV -

30 November 2018

This contribution is submitted by South Africa under Session IV of the Global Forum on Competition to be held on 29-30 November 2018.

More documentation related to this discussion can be found at: oe.cd/invpw.

Please contact Ms. Lynn Robertson [E-mail: Lynn.Robertson@oecd.org], if you have any questions regarding this document.

JT03440521

Investigative Powers in Practice

Breakout Session 1: Unannounced inspections in the digital age

- Contribution from South Africa-

1. Introduction

1. In South Africa the unannounced inspections or search and seizure operations are regulated by section 46 and 47 of the Competition Act 89 of 1998. Section 46 provides for the authority to enter and search with a warrant while section 47 provides authority to enter and search without a warrant, if there are reasonable grounds to believe that a warrant may be issued if applied for.

2. The Commission can seize both hard copies and electronic data during the unannounced inspection. The hard copies are seized by Commission inspectors while the electronic data is seized by outsourced IT forensic experts.

3. In the past, the Commission used summons and information request letters extensively as a tool to collect evidence of collusion. For the past five years the Commission utilised unannounced inspections more frequently to collect evidence of cartel infringement.

4. In 2014/2015 financial year, the Commission conducted four (4) unannounced inspections, in 2015/2016 financial year five (5) unannounced inspections, In 2016/2017 financial year four (4) unannounced inspections and in 2017/2018 financial year three (3) unannounced inspections. The Commission also utilised summons and information request letters as tools to collect evidence of collusion.

5. During unannounced inspections, the Commission seizes electronic data contained in computers, servers, mobile phones, laptops and other electronic storage devices. In order to illustrate the challenges that the Commission encounters when dealing with electronic data both during and after the dawn raid, a case study concerning an actual market in which the Commission has conducted a dawn raid is presented below.

2. Breakout Session 1: Unannounced inspections in the digital age

6. The Commission through independent IT forensic experts clone or image the electronic devices and seize in sealed evidence bags during the search and seizure operation. This data is taken to custody by the independent IT forensic experts. The data will then be search by the independent IT forensic experts using key words provided by the Commission. The legal representatives of the firms that are subject of the investigation will provide key words to the independent IT forensic experts to identify and extract privilege information from the information extracted using the Commission key words.

7. The challenges of collecting electronic data during unannounced inspections which the Commission has encountered include:

- Large volume of data;

- Laptops not in the identified premises;
- Servers hosted in third party premises not covered in the warrant; and
- Electronic data stored in cloud.

8. The challenges relating to large volume of data are that it takes longer time to image, process and search using key words. It also take longer time to identify and extract privileged information. This is also costly as it requires more time spent on it.

9. The Commission has addressed this challenges by narrowing down the key words for searching the relevant evidence and use software that is able to further refine the key word searches.

10. The challenge relating to laptops not in premises is that the respondent often argue that such laptops are not cover by the search warrant. The Commission address this challenge by ensuring that the scope of the warrant covers even devices that are relevant but are located outside the premises.

11. Often the server are located outside the specified premises to be searched. This pose a challenge that the Commission cannot access such servers as the search warrant is limited to the specified premises. The Commission address this challenge by expressly stating such eventuality be covered in the search warrant. Sometimes judges refuse to grant order authorising the Commission to image off site server but they make provision to telephonically apply for permission to enter premises where such servers are located.

12. The challenge with electronic information stored in the cloud server is that the information cannot be imaged. Instead, one can only extract the relevant information directly from the cloud server. The information is usually extremely voluminous. This method is also extremely expensive as the relevant information is extracted with key words using internet connection. If network coverage is slow, the extracting of the information can take longer to complete.

13. Further, you have to rely on the respondents to give you log in details to access the electronic information. The only way the Commission address this challenge is by having refined key words during the search operation.