Organisation for Economic Co-operation and Development

DAF/COMP/GF/WD(2018)18

Unclassified

English - Or. English

20 November 2018

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Global Forum on Competition

INVESTIGATIVE POWER IN PRACTICE – Breakout session 1: Unannounced Inspections in the Digital Age – Contribution from Australia

- Session IV -

30 November 2018

This contribution is submitted by Australia 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.

JT03439928

Investigative Powers in Practice

Breakout session 1 - Unannounced Inspections in the Digital Age

- Contribution from Australia –

1. Introduction

1. This paper discusses challenges that the ACCC faces in exercising its investigative powers arising from the widespread digitisation of information. It explores processes established to manage these issues, as well as the opportunities presented by the availability and accessibility of data.

1.1. Dawn raids and digital evidence

2. With ever-increasing amounts of data being stored electronically by businesses, the ACCC has, and continues, to adapt its approach to obtaining that information. Search warrants and other compulsory information gathering exercises often result in agencies needing to sort through vast quantities of electronic data to identify relevant material. Electronic searches create their own challenges, some of which can be dealt with in the pre-planning stage, while others, like the handling of legally privileged documents, require different methods to physical document management.

Pre-planning to make electronic searching during an unannounced inspection more effective

1. The challenges associated with obtaining evidence in the digital age are amplified in the context of an unannounced inspection (also referred to as a 'dawn raid' or 'raid'). The following are some steps that the ACCC has used to make raids involving digital material more efficient and effective:
    - Prepare a detailed IT plan prior to seeking a search warrant in conjunction with external (government or commercial) IT consultants. Such a plan may identify key targets, prioritise devices and consider potential issues.
    - Prepare effective search keywords, including unique words and 'search strings', to enable accurate and efficient identification of relevant documents. Keywords should be provided to forensic IT consultants in advance for feedback and to pre-load them into the search software.
    - Have the forensic IT consultants demonstrate software to be used during the raid to the agency staff assisting in the raid, so as to ensure familiarity.
    - Prepare documents to seek an order requiring a person to provide assistance if, for example, administrative credentials are required to access evidence.
    - Prepare legal privilege protocols (discussed below).

Dealing with legal privilege issues

2. In Australia, legal professional privilege (LPP) protects communications between clients and their legal advisors if those communications were confidential and made for the dominant purpose either of giving or receiving legal advice, or for use in existing or anticipated litigation.[1] It protects those communications from any compulsory disclosure including through subpoenas, search warrants (similar to dawn raids) and document requests from agencies like the ACCC.[2]

3. To deal with legal privilege issues in electronic document seizures, the ACCC engages an independent third party to host the electronic data and remove the privileged material before it is reviewed by ACCC investigators.

4. The ACCC usually seeks to enter into an agreement with the occupier of premises subject to a search warrant, which sets out the process for claiming privilege on electronic material.[3] The current LPP Agreement template states that the occupier will provide a list of privileged material, including particular metadata, and the grounds for claiming privilege.

5. One challenge with this process is that it may be difficult to identify and exclude the privileged material during searches conducted over the material by the third party hosting the data subsequent to the warrant being executed. A possible solution to this is for the agreement between the ACCC and the occupier of the premises to include a requirement that the occupier identify privileged documents by providing electronic native copies of the actual files to the independent third party hosting the data. Forensic techniques can then be used (in the period after the search) to accurately identify the documents in the dataset and remove them as well as any duplicates of these documents, before uploading the balance for review.

Case study – alleged cartel investigation

6. The following is an example of how an unannounced inspection into an alleged cartel was prepared and conducted by the ACCC.

7. At the pre-planning stage, an IT search plan was prepared to prioritise devices and the digital locations of evidence according to our estimate of their most likely locations, e.g. certain parts of a server, mailboxes and personal computers/devices used by particular individuals. Desk-based research was also conducted in relation to the target company's IT infrastructure (e.g. the likely use of cloud-based email servers).

8. In this case, the ACCC engaged an IT forensic service provider from another government department; in other cases, the ACCC might engage a commercial firm. The ACCC worked with the IT service providers to create a keyword search list that was based on the names of companies and individuals involved, as well as unique terms relating to possible price fixing and market sharing agreements.

9. On the day the warrant was executed, after effecting entry and ensuring there were no safety issues, a floor walk was conducted and all employees were asked to step away from their computers and leave personal devices on their desks. ACCC 'IT search staff' then identified all IT devices on the premises, and catalogued and triaged them in terms of importance. Devices were then provided to the IT service provider, in a triaged order, for searches to be run.

[1] *Esso Australia Resources Ltd v FCT* [1999] HCA 67 [61].

[2] Daniels Corporation International Pty Ltd v ACCC [2002] HCA 49 [37] determined that the ACCC's power to compel the production of documents via section 155(1)(b) of the Competition and Consumer Act 2010 (Cth) did not override the protection of legal professional privilege.

[3] Although not required, in the first instance the ACCC will offer the occupier the option of entering into an agreement. If the occupier ultimately did not agree, the ACCC would give them a copy of the protocol that would be used.

- Australian search warrant legislation overrides privacy legislation for personal mobile devices, which means the ACCC can examine personal devices for material relevant to the warrant. However, we use a common sense approach – if we determine that a person is unlikely to have information on their device that is relevant to our investigation, we will often decide not to examine the device and return it to the owner.

10. In this case, as soon as the premises were secured, the executing officer requested the contact details of the company's IT manager. This was arranged, but with a delay due to the IT manager being offsite and the intervention of company lawyers.

11. ACCC IT search staff were responsible for reviewing all responsive documents relative to keyword searches, and bringing them to the attention of the executing officer for a decision about which material should be copied.

    - For example, upon finding relevant material in an employee's email account, the ACCC copied the .pst file of the whole mailbox to preserve the forensic integrity of the mailbox including metadata, calendar entries and mail for subsequent consideration off-premises. In other cases the ACCC copied folders which contained relevant documents from the target's server.

12. In accordance with the process outlined above, it was agreed that the company could make LPP claims directly to the third party IT provider so that LPP material could be removed before the ACCC's review.

13. It took 24 hours to execute the warrant. The main delays involved locating the right person to provide access and information about the network infrastructure, running searches across cloud-based servers and mailboxes, copying data from various locations (including the cloud, which can be very time consuming), and agreeing on the LPP process.

Call charge records

14. The ACCC can covertly access historical telecommunications data about individuals held by telecommunications carriers in Australia.[4] Due to the obvious privacy implications for individuals, ACCC staff must ensure that any request for access to telecommunications data is justifiable based on the allegations made and the likely value of the information being sought.

15. In cases where telecommunications data – specifically, call charge records (CCRs) – is obtained, the data can be used to investigate and provide evidence that is beneficial to an investigation.

16. CCRs provide details relating to calls made from, and calls received by, a specific number over a specified period.

17. The ACCC can only access the metadata from CCRs, not the actual content of the calls. However, the metadata can provide useful information. For example, CCRs can:

    - corroborate an allegation
    - show the target's network – who they are communicating with and how frequently
    - identify the physical location of the target's mobile telephone at the time it was used to make or receive a call or message

[4] Under the *Telecommunications (Interception and Access) Act 1979* (Cth), specified government agencies, including the ACCC, can request access to certain existing telecommunications information or documents if it relates to either the enforcement of the criminal law (s178) or enforcement of a law imposing a pecuniary penalty (s179).

- support a 'pattern of life' analysis
- reveal the timing of calls around specific events
- reveal specific patterns of calls (e.g. that may suggest collusive conduct).

Case study – construction industry cartel investigation

18. An investigation was initiated by an anonymous complaint alleging collusive activity over a three year period, with the names of two individuals and companies provided. ACCC investigators requested three years of CCR data on both individuals' mobile phones. Initial CCR research showed a high level of communication between these individuals.

19. The ACCC's Strategic Data Analysis Unit then developed a program which identified instances of potential meetings based on CCR data based on the times and locations of calls. This revealed four potential meetings and identified two other potential meeting participants. On the call timelines, for example, it was shown that Target A called the New Target, before immediately calling Target B, who then, later that day, also called the New Target who was a manager in a competing company.

20. This case shows that CCRs can give useful insights for competition investigations. Supported by other evidence, CCRs can also provide a basis and justification for further investigative strategies, including applications for warrants, physical surveillance and compulsory interviews.