International Chamber of Commerce
The world business organization

ICC Recommended Code of Practice for Competition Authorities on Searches and Subpoenas of Computer Records

Commission on Law and Practices Relating to Competition, 16 October 1998

Introduction

The increasing use of information technology to coordinate and facilitate business operations and relationships across national borders is giving rise to significant competition law enforcement challenges.

Competition law authorities have responded to these challenges through the use of sophisticated and flexible computer search law enforcement tools to review and collect electronic data. How ever, computer searches initiated in one jurisdiction may impinge on the territorial sovereignty of another and may require that competition authorities in one jurisdiction coordinate their enforcement activities with those of their counterparts in other jurisdictions.

Business have a number of growing concerns about the use of computer searches by competition authorities. These concerns include:

- protection of confidential data (business concerns about ensuring adequate safeguards for confidential and competitively sensitive data provided to or seized by competition authorities are discussed in ICC Statement on International Cooperation between Antitrust Authorities (28th March 1996, Document no 225/450 Rev. 3);
- the loss of time and disruption of business while computer records are being searched;
- the risk of loss or destruction of data and allocation of liability for damage; and
- the risk of inadvertent disclosure of third party documents (for example, where the company being searched is linked to a business partner).

There is no well-developed body of case law to provide guidance on the issues arising in this area. Given the volume of computer records generated by most businesses, there is an urgent need to ensure that enforcement practices and policies reflect a clear understanding of how computers work, how businesses use them, and the extent to which traditional approaches to the collection of computer records may unnecessarily impose significant costs on business.

ICC has developed this recommended code of practice to provide guidance to governments seeking to respond to these challenges. The recommended code of practice should be read in conjunction with the ICC Policy Statement on International Cooperation between Antitrust Authorities (26 March 1996; doc.no. 225/450 Rev 3), and the ICC GUIDEC (General Usage for International Digitally Ensured Commerce)(1997).

Background

Computer records are typically stored, in digital form, on either magnetic or optical media. Such records may either be stored online, which means they are accessible from a computer without any requirement for human intervention, or offline, in which case the relevant media must be physically loaded on a computer system by a human operator before the records may be accessed. Computer records may be transmitted using a variety of wireless or wireline telecommunications facilities[1]. Firms frequently use such telecommunications facilities to connect computers in different locations, in the same or different countries.

International Chamber of Commerce
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 29 42
E-mail icc@iccwbo.org Website www.iccwbo.org

Computer systems contain a number of automatic mechanisms which help ensure that the systems function smoothly, permit accidentally deleted information to be retrieved, allow information to be shared among several users, and enable other features. These mechanisms frequently generate multiple copies of documents, and fragments (pieces) of files which lack the contextual information required for the reader to understand their meaning.

Search warrants and subpoenas authorizing the seizure or collection of documents or computer re cords are typically issued only after a judge or other official has been satisfied that the competition authority's request meets the applicable legal requirements, which are designed to protect privacy interests and to ensure that the proposed seizure or collection is otherwise reasonable. The review and seizure of computer records may be viewed as unreasonable if the scope of the information seized exceeds that reasonably contemplated by the judge issuing the order, or the search warrant or subpoena imposes unreasonable burdens on the subject firm. The law and practice in this regard is reasonably well-developed with respect to paper records, but less so with respect to computer records.

In the European Community, the practice of the Commission is to execute search warrants which it has itself issued. Such warrants are in theory justiciable before the European Court of Justice but, given the Commission's practice of implementing so-called "dawn raids", it is rare that the Luxembourg Court is able to determine the reasonableness or otherwise of the warrant in question.

Issues Concerning the Seizure of Computer Records

Some of the issues arising out of the seizure of computer records, or subpoenas requiring their production, include:

- the protection of computer systems and stored computer records from damage during searches by competition authorities;
- the allocation of liability for any damage caused to computer systems or computer records during the searches by competition authorities;
- the authenticity, integrity and reliability of seized computer records and the processes and procedures which should be employed to document and verify same;
- the treatment of deleted files, file fragments[2], temporary files and other artifacts created by computer systems in the normal course of their operations;
- the treatment of documents belonging to third parties which are inadvertently accessed through a link between the computer system of the company being searched and the third party;
- the implications for computer searches of technological developments such as the use of replication, dynamic data links, and object-linking and embedding or other similar technologies (which are used to link or reproduce information contained in one file to a second file);
- the protection of information which is subject to legal privilege during the seizure of computer records or file fragments;

- the ability of the authorities to compel the subject firm to assist in the search of the computers located at the facility by providing access to software or passwords or other technical information, including encryption keys;

- the ability of the authorities to compel the subject firm to assist in the search of computers located at other facilities by providing passwords or other technical information, including encryption keys;

- the ability of the a uthorities in one jurisdiction to access or seize information stored on computers in other jurisdictions; and

- the ability of the authorities in one jurisdiction to share confidential information with authorities in other jurisdictions (see ICC Statement on International Cooperation between Antitrust Authorities.)

The ease with which computer records may be created or modified raises further issues with respect to the probative value of different types of computer records. For example, the probative value of information contained in a file fragment may be limited by the absence of the other parts of that file and information respecting the context in which the file was created. Further, and in some respects more fundamental, issues arise as a consequence of the relative ease with which computer data may be modified.

In this context, ICC recommends that the following guidelines be observed by competition authorities with respect to searches or subpoenas of computer records.

Suggested Guidelines

When requesting or issuing a search warrant or a subpoena, the competition authority should:

- consider whether the seizure of computer records is required (e.g., would the search provide new evidence or merely additional copies of documents that are available in paper form);
- if computer records are required, consider whether the seizure or production of all such files is required. As a general rule, the authority should avoid asking a firm to produce multiple copies of the same document or to take steps that would require it to stop using its computers to comply; and
- consider, or bring to the attention of the judge or other officer issuing the search warrant or subpoena:
    - - the range of the computer files that will be subject to the warrant or subpoena and the steps the firm will need to take to comply (e.g., whether the order will likely require the firm to stop using its computers); and
    - - the possibility that the subject firm's computers may be linked to locations outside that named in the warrant or subpoena.

When executing a search warrant that authorizes the search and seizure of computer records, the competition authority should:

1. before using a firm's computer, ask whether the computer is linked to other locations or provides access to information owned by third parties. If there are other locations in the same jurisdiction,

additional search warrants should be obtained before data is seized from such locations. Similarly, competition authorities should not use the subject firm's computer to access or seize a third party's data without either the voluntary cooperation of the third party, or the issuance of another search warrant relating specifically to the third party's data;

2. competition authorities sh ould not use the firm's computers to access or seize information stored on computers outside their jurisdiction. Rather, existing procedures (e.g. those available under applicable mutual legal assistance treaties and legislation) through which the local competition authorities are asked to gather such information, should be used in the same manner as with other forms of information located in foreign jurisdictions;

3. in consultation with the subject firm, develop and observe procedures to minimize the likelihood of damage to the firm's hardware, software, data or operations;

4. avoid removing computer hardware where such seizure would disrupt the business of the firm or others with which it does business. If necessary, the competition authority could seal and investigate the hardware in the presence of the subject firm;

5. in consultation with the subject firm, develop and observe procedures to maintain the status of privileged materials and avoid disclosure thereof;

6. be held accountable for any harm to the subject firm's property or business that results from a search that failed to observe the foregoing guidelines;

7. where the competition authority and the firm cannot agree with respect to the foregoing, seek instructions from a court rather than acting unilaterally;

8. where possible, make copies of computer records where the seizure of original records would disrupt the business of the firm or others with which it does business. With respect to such copies, develop and document the mechanisms that are used to ensure that copies of the computer files are true and accurate copies; and

9. comply with the safeguards prescribed for the protection of business information in the ICC Statement on International Cooperation between Antitrust Authorities.

(1) These include public switched telephone networks, analog or digital private lines, virtual private lines, packet switched networks (including Internet and asynchronous transfer mode networks), short range infrared devices, analog and digital cellular, personal communications services (PCS), local multipoint communications services, two-way radio, terrestrial microwave and various forms of digital and analog satellite communications services.
(2) The identification and collection of potentially relevant file fragments is unlikely to result in the seizure of significant information. Since file fragments frequently contain remnants of unrelated temporary files, in many cases they are unintelligible.

Back to ICC statements and rules
Back to Rules