Organisation for Economic Co-operation and Development

DAF/COMP/GF(2018)7

Unclassified

English - Or. English

23 October 2018

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Cancels & replaces the same document of 23 October 2018

Global Forum on Competition

INVESTIGATIVE POWERS IN PRACTICE – Break-out session 1: Unannounced Inspections in the Digital Age

- Issues Note by the Secretariat --

30 November 2018

This document was prepared by the OECD Secretariat to serve as an issues note for the Break-out session 1 on *Unannounced Inspections in the Digital Age* for Session IV at the 17th Global Forum on Competition on 29-30 November 2018.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

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

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

JT03438046

Table of contents

Investigative Powers in Practice Break-out session 1 - Unannounced Inspections in the Digital Age3

1. Introduction 3

2. Advantages and Disadvantages of Digital Evidence Gathering 3

3. Principles and Practice of Digital Inspections 4

3.1. Principles of Digital Forensics 4
3.2. Practices and Methods 5
3.2.1. Collection 5
3.2.2. Preservation 6
3.2.3. Analysis 7

4. Challenges of Digital Evidence Gathering 7

4.1. Power and capacity to gather digital evidence 7
4.1.1. Legality 7
4.1.2. Capacity 10
4.2. Privileged Information 10
4.3. Privacy and Data Protection 10
4.4. Location of the Digital Information 12
4.5. Transparency 12

5. Conclusion 13

Endnotes 14

References 16

Boxes

Box 1. Incidental Evidence 9
Box 2. Inspection of Personal Mobile Devices – A Case from Spain 11

Investigative Powers in Practice

Break-out session 1 - Unannounced Inspections in the Digital Age

1. Introduction

1. Today information is produced, stored and processed mainly in digital form. Communication is facilitated increasingly by digital technologies such as e-mails and mobile instant messaging apps. Daily global e-mail traffic is estimated to surge from 182.9 billion in 2013[1] to 281.1 billion in 2018[2]. The number of instant messaging accounts (not including mobile messaging) rose from 3.3 billion[3] to 6.4 billion[4] in the last three years. This not only affects private communication but also business communications. Companies digitalise their business processes such as payments, stock management and data storage for its many benefits including efficiency, innovation and security.

2. Digitalisation also has its impact on competition authorities' unannounced inspections. The power to conduct on-the-spot inspections is probably the most extraordinary tool of competition authorities to gather evidence and information.[5] In the digital age, this tool would benefit extremely from the capacity to effectively search digital media and to collect digital evidence.

3. This note presents the main issues related to digital searches in unannounced inspections. Section 2 discusses advantages and disadvantages of digital evidence gathering. Section 3 focusses on principles and methods of digital inspections. Section 4 outlines various challenges faced by competition authorities regarding digital evidence gathering, and finally, section 5 concludes.

2. Advantages and Disadvantages of Digital Evidence Gathering

4. Digitalisation has many benefits for its business users, including enhanced security through encryption, greater accessibility and higher efficiency. For competition agencies, digitalisation of business processes offers a wealth of advantages as well.

5. Firstly, digital evidence gathering broadens the potential sources of evidence. Today, almost all information is created or processed in a digital environment or transferred to a digital medium. Often this information does never even exist in hard-copy (ICN, 2014, p. 7[1]). In this context, digital search provides competition authorities with better chance of discovering evidence during unannounced inspections.

6. Secondly, digital evidence is sometimes harder to destroy compared to physical evidence. The digital environment presents the opportunity to retrieve deleted or damaged data. Even if a document on one digital medium is destroyed permanently, it can be found on other digital media or leave traces of existence so its destruction can be detected more easily.

7. Thirdly, information on a digital document, unlike physical evidence, is not limited to its content. Information about the data itself, which is called metadata, can also be valuable for an investigation. Metadata may contain information such as origin of the document, the author of the document, date/time created/altered/deleted, the last update date, persons who accessed the document, or the identity of sender or receiver (ICN, 2014,

p. 7[1]). For instance, the cartel screening tool developed by the UK Competition and Markets Authority uses document authorship metadata, among other criteria, to detect tender documents which may have the same origin, and therefore signifies a higher likelihood of bid rigging.[6]

8. Finally, digital evidence may prove more useful in case management and digital search systems. Documents in their native format are likely to return more comprehensive search results compared to scans of hard-copy documents (ICN, 2014, p. 8[1]).

9. There are also challenges related to digitalisation of business processes. Digital data may be more vulnerable than physical documents. They can be altered or destroyed by the daily operation of IT systems or physical conditions (e.g. high temperature and electromagnetic fields). Therefore digital evidence collection requires special care in terms of security and preservation of the data.

10. Digital evidence gathering also requires additional expertise, tools (e.g. equipment, software) and infrastructure (e.g. rooms dedicated to forensics). Building and maintaining digital evidence gathering capacity is more costly than conventional evidence gathering capacity.

11. Finally, in many jurisdictions, the legal framework does not contain specific rules regarding digital evidence gathering and the rules relating to physical evidence collection cannot be directly adapted to digital evidence issues. This situation decreases legal certainty for competition authorities and other relevant parties.

12. Nevertheless, there cannot be any doubt that digital evidence collection is becoming more and more indispensable and needs to complement the still relevant collection of physical evidence in order to have an effective law enforcement regime.

3. Principles and Practice of Digital Inspections

13. Increasing number of the competition authorities include digital data in their inspections to find relevant evidence. The methods and procedures adopted by the competition authorities differ to a great extent depending on their resources and the relevant legal framework. Some principles regarding digital evidence gathering seem to be widely accepted and can help shape the practice of digital inspections.

3.1. Principles of Digital Forensics

14. Digital forensics, whihc is a branch of forensic science, encompasses the application of scientific techniques for identifying, preserving, recovering and analyzing the digital information and presenting facts and opinions about it. Digital forencics respects legal standards of admissible evidence and relevant legal procedures. There are established principles in the digital forensic discipline regarding digital evidence gathering. These principles include the following:

- Legality: All digital information should be collected lawfully (ICN, 2014, p. 17[1]). In this sense, digital inspections should have a legal basis. Moreover, digital inspections should be carried out within the boundaries drawn by the inspection decisions or court warrants and the subject matter of the case.
- Competence: Digital evidence gathering requires expertise and diligence. “Persons conducting an examination of digital evidence should be trained for that purpose”

(US DoJ, 2004[2]). All officers involved in digital evidence gathering process should know the procedures (ICN, 2014, p. 17[1]).

- Integrity and security: Actions taken by law enforcement agencies, their employees or agents should not change the data while securing, collecting and analysing it (US DoJ, 2004[2]) (APCO, 2012[3]). The data should be preserved to such an extent that a third party can replicate the same result as presented to a court (APCO, 2012, p. 7[3]).
- There are physical and digital security measures to be taken by the personnel who gather evidence. For instance, it is a good practice to work on copies of the original evidence in order to prevent destruction, damage or alteration of the original data (ICN, 2014, p. 23[1]). If a person has to access original data, "that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions" (APCO, 2012, p. 1[3]).
- Authenticity: Authenticity of evidence shows its provenance and genuineness. In order to establish authenticity of digital evidence, it is crucial to maintain a chain of evidence[7] and chain of custody[8]. Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review (US DoJ, 2004[2]). This record of all processes applied to digital evidence should be available to an independent third party to examine the original data following the same steps and to reach the same results (APCO, 2012[3]). In this sense, integrity and security of the original data are musts for replicability and they are integral parts of authenticity.

15. Although these principles are articulated specifically for forensic processes, they are based on the rules related to admissibility of an evidence and also relevant for other more basic digital evidence gathering practices such as keyword searches on an e-mail account. These principles help competition authorities to design better practices for their digital evidence gathering efforts.

3.2. Practices and Methods

16. Inspection methods and practices vary among jurisdictions for a number of reasons, including available sources (e.g. equipment, software, trained staff) or the legal framework. Some authorities cannot collect digital evidence stored on mobile phones or cannot take forensic images (ECN, 2013[4]). In such cases authorities deploy rather simple conceptual searches on the inspected media by using inbuilt search tools. Others use advanced forensic tools and techniques.

17. Yet all types of digital inspections are composed of stages such as planning, identification of relevant digital evidence sources, collection of evidence, preservation of evidence during all the processes, analysis of the data, and the presentation of the evidence. However collection, preservation and analysis of digital information constitute the most important aspects of digital inspections for competition authorities.

3.2.1. *Collection*

18. The collection of digital evidence is at the core of legal discussions as the most crucial point in the management of digital evidence (Kasper and Laurits, 2016, p. 197[5]). Mishandling data at this stage can lead to destruction of evidence or its inadmissibility.

19. In unannounced inspections, digital data is collected mainly in two ways. The first is the physical seizure of the data carriers such as hard drives and CDs. Seized data carriers

then searched for relevant evidence in the premises of the authority. At this stage deleted or damaged data can be retrieved by forensic tools. During sifting of evidence, only information protected by legal professional privilege is excluded from the process.

20. The second way is searching the data carriers on the premises of the inspected undertaking and copying or making forensic images of the digital data. Some authorities also engage in live forensics[9] to capture volatile data which cannot be accessed once the device is turned off (ICN, 2014, pp. 10, 22[1]).

21. Forensic IT tools are not used by every competition authority to collect digital evidence. In cases where forensic tools are not used, digital sources of evidence are searched through inbuilt search tools and deleted data is retrieved from "recycle bins" or backup servers.

22. At the collection step, some measures should be taken by the inspection teams to ensure the integrity of the data and to enable authentication. For instance, when imaging data carriers, write blockers are used to secure the integrity of the source media. Hash values[10] of every copied/imaged data are generated to enable verification that the copy is identical to the original digital information. It is also important to document every action during this process.

23. Once the digital data gathered, some authorities transport the data to their premises (or to premises of police or an equivalent enforcement authority) to continue searching of this information. This procedure is called continued inspection procedure. Some authorities sift the digital evidence on a *prima facie* basis at the premises of the inspected party and conduct further review at the premises of the authority. In some variations, complete sifting of the digital evidence at the investigated premises (ECN, 2013, pp. 3-4[4]) (ECN, 2012, p. 14[6]). In these cases, only a selection of copied information is taken away to the competition authority for the case handling team (ICN, 2014, p. 10[1]). Some authorities use both procedures alternatively, depending on the specificities of the case.

24. The ECN (2012[6]) recommends a continued inspection procedure as an effective way of digital evidence gathering. This procedure grants more time to further search the data and better understand the case so increases the possibility to detect relevant evidence in the often voluminous digital case file. In addition, this procedure minimises the disruption of the undertaking's operations. However, it is also argued that copying and taking away a huge amount of data for review/sifting potentially risk the violation of an basic rights such as privacy or violations of legal privilege (Michalek, 2015, p. 205[7]).

25. Sifting the digital data at the investigated premises has its advantages and disadvantages, too. On the one side, this procedure enables the company to directly claim privilege for some information. Case team can access the selected data in relatively short period of time. On the other side, case team cannot go back to the copy/image of the digital evidence source and "have to be contend with the selection at the premises of the company, even if new intelligence develops during the investigation" (ICN, 2014, p. 10[1]).

26. At the end of selection process, non-relevant digital information is either returned to the company or deleted permanently (ICN, 2014, p. 21[1]).

3.2.2. *Preservation*

27. Preservation is the prevention of deletion or destruction of the digital evidence during an inspection, transportation and examination. Preservation measures include leaving devices running for live forensics, requesting blocking access to mailboxes at the

server level, unplugging network cables from the computers to avoid access, protecting data carriers from static electricity, magnetic fields and concussions. As mentioned previously, processing working copies of the digital data is a widely accepted measure to avoid accidental harm to the original digital data. Maintaining a sound chain of custody until the closure of the case is also crucial.

3.2.3. *Analysis*

28. Analysis is the step where forensics experts or/and the case team conduct an in-depth examination of the data to find pieces of evidence that shed lights on the subject-matter of the investigation. Reviewing all the data one by one is not a realistic option. Since digital searches can yield huge amounts of data, some kind of search strategy needs to be developed. Keyword searching is the most used method (ICN, 2014, p. 24[1]). Keywords are derived from desk research, informants, leniency applicants or explanations sought during the on-the-spot inspection. As analysis progresses, new keywords can be added to the list. Specially developed forensic search software can identify misspelled versions of the keywords and yield more comprehensive results, as well as produce results on the basis of self-learning algorithms.

29. Other analytical methods are confirming user attribution, viewing the print spooler, testing file signatures to find bad file signatures, searching for encrypted information, investigating traces of web chats, webmail and so on (ICN, 2014, pp. 24-25[1]). Applying more than one method to the data can minimise the risk of false negatives.

30. A notable lack of digital data can also be relevant to the analysis. For example, "extremely few or no e-mails during a certain period of time or from a certain employee" (ICN, 2014, p. 25[1]) can inform the analysis as well.

31. It is again important to document all the action taken to extract the evidence to maintain chain of evidence, to enable third parties to reproduce the same results.

4. Challenges of Digital Evidence Gathering

32. Digital inspections transfer control over an immense amount of data from undertakings to competition authorities, and the technology used by inspected parties and competition authorities develops constantly. This creates legal as well as technological and practical challenges to competition authorities, which will be discussed in this section.

4.1. Power and capacity to gather digital evidence

33. Competition authorities need a legal ground to collect digital evidence. When the legal criteria are duly met, the authorities also necesitate the technical capacity to conduct digital inspections.

4.1.1. *Legality*

34. Competition authorities cannot gather digital evidence without a legal basis. Currently almost all the competition authorities derive their power to gather digital evidence from the already existing power to review all the books and records of the inspected undertaking (ICN, 2014, p. 26[1]). The usual interpretation is that regardless of its form, all the information on the premises of the company is subject to inspection.

35. The power to conduct digital search is not without limits. As in the case of any unannounced inspection of physical evidence, a digital inspection must be proportionate and within the scope of investigation to be lawful. However, methods and procedures applied in digital searches can raise particular question as regards the interpretation of these limitations.

36. When hard drives are seized for future search or the server of the company is copied almost entirely, this may result in the unintended seizure of information falling outside of the legitimate scope of the inspection decision or warrant. This practice can raise proportionality concerns in some jurisdictions. Competition agencies seek to mitigate these concerns by applying search tools and keywords that shall ensure that only those data will be picked that have a reasonable nexus to the investigation. Since the competition authority can be deemed going beyond what is necessary and reasonable to achieve its legitimate goal.

37. In cases where a search tool is used to determine which data to be copied, relevance may be still an issue. It is argued that the search terms must not be too broad to ensure that only results within the scope of the inspection decision are produced (Lang, 2014[8]) (Polley, 2013[9]). The concern is that inspections can otherwise turn into "fishing expeditions". There are concerns that overly intrusive digital searches increase the risk of an illegal use of information which is accidentally gathered by asserting that the information was only treated as "intelligence", not as evidence (Michalek, 2015, p. 205[7]).

38. Strong procedural safeguards can mitigate proportionality and relevance concerns. Judicial review which fulfils a genuine supervisory function can protect the rights of inspected parties effectively. In some jurisdictions such as Germany, India and the US, unannounced inspections are subject to ex-ante judicial review. No matter how strict ex-ante review is, ex-post judicial review is indispensable. Ex-post judicial review can be either on stand-alone basis or retrospective, meaning that procedural decisions can be reviewed only within the context of a final decision regarding the case. Lack of stand-alone judicial review of unannounced inspections is criticised because it could deny the inspected party an appropriate remedy (Jalabert-Doury, 2009, p. 8[10]) (Michalek, 2015, p. 208[7]).[11]

39. Another legal issue is often raised with regard to the company representative's right to be present during the subsequent searches of the copied data. In some jurisdictions such as Austria, sifting of the copied or imaged data takes place at the premises of the authority without presence of the representatives of the inspected parties. In other jurisdictions (e.g. Danmark, the EU, the Netherlands), representatives of the inspected party are invited to attend subsequent search of the imaged or copied data (Jalabert-Doury, 2009[10]). In order to facilitate observance of inspected party on the extended inspection, a list of key words used when analysing the data or a copy of selected evidence may be provided. Still some authors criticise continued inspection procedure arguing supervising prolonged searches may impose a heavy burden on inspected parties with limited sources (Simonsson, 2013, pp. 10-11[11]) and the inspected party must have a genuine choice on place of inspection (Michalek, 2015, p. 210[7]).

Box 1. Incidental Evidence

Incidental evidence can be described as "any evidence found incidentally in the course of an inspection and relating to suspected infringements of competition rules not covered by the initial inspection decision" (ECN, 2013, p. 20[4]). While several competition authorities can secure or seize incidental evidence during an inspection, others would need a new authorization to inspect. For instance, the Court of Justice of the European Union ruled that the EU Commission cannot seize or copy evidence out of the inspection's scope intentionally[12] but can initiate a separate "inquiry in order to verify or supplement information which it happened to obtain during a previous investigation if that information indicates the existence of conduct contrary to the competition rules".[13] Whereas Hungarian Competition Authority[14] (GVH) can seize incidental evidence and seek approval of judicial body subsequently. In 2007, Appeal Court of Budapest upheld an infringement decision of the GVH concluding that "the GVH lawfully used the evidence, which it obtained in another proceeding"[15].

Since digital searches enable access to a great amount of information during unannounced inspections, incidental evidence issue may come up more often. The judgement of the Swedish Market Court on the incidental evidence in the context of digital inspections was one of these cases. In November 2013, the Swedish Competition Authority (KKV) opened an *ex officio* investigation regarding ASSA's conduct in the Swedish market for locksmith wholesale services. The KKV conducted an inspection at the premises of two subsidiaries of ASSA ALBOY Group (ASSA Group) and removed copies of digital information with the consent of inspected party[16] to further examine the data at the authority's premises.

During the analysis, the KKV chanced upon information about a separate potential infringement which was not covered by the initial inspection warrant. Therefore the KKV applied to Stockholm District Court for an authorisation to expand the search on the already collected data. In March 2014, the court granted the KKV the requested authorisation. The ASSA Group appealed to the Swedish Market Court, arguing that KKV's request was not supported by the law and that ASSA's consent to remove the electronic data had been limited to the initial scope of the warrant.

The KKV asserted that ASSA's consent was merely about the place of the search and that this would not limit the scope of the search. The KKV also argued that information found incidentally could be the basis to request search power in the context of a separate investigation, and underlined that searching the data already seized is more efficient than launching a new inspection or sending a request for information. The KKV highlighted the fact that company representatives could be present during an extended review at KKV's premises. The KKV also presented the difficulty of gathering information as a justification for extended search. The KKV also argued that ASSA had already withheld crucial information during a merger case in 2013 and that this risk was still valid in the current case. Therefore if a new inspection had to be launched, it was crucial for the KKV to be able to cross-check the information with the already seized data.

In 2015, the Market Court ruled that there was no legal ground for an extended search on the seized data since Swedish Competition Law mentions inspections "at companies' premises" and the KKV's power to remove copies of electronic data to KKV's own premises for review was not certain. The Court stated that such consent to data removal is not a *carte blanche* to the KKV to search at will but that it is rather limited to the scope of the particular inspection. Under the Swedish Competition Law, an on-the-spot inspection is allowed when less burdensome options are not viable and there is a risk that evidence would otherwise be withheld or distorted. It is also decided that the case in question would not meet these preconditions since the KKV was seeking permission to further search digital evidence it already held and over which ASSA had lost control.

Sources: Suspected anti-competitive conduct – investigation related to the market for locksmith wholesale services, Presss Release by KKV, *http://www.konkurrensverket.se/globalassets/english/competition/13-0494-english.pdf.*
Setback for Electronic Searching by Swedish Competition Authority, *https://www.nordiccompetitionblog.com/?p=494.*

4.1.2. *Capacity*

40. Digital inspections require specialised staff, facilities allocated to the analysis and preservation of digital data and technical equipment and software. As technology advances, these capacities must be constantly updated and enhanced.

41. It is recommended to have an internal unit or group of staff which is capable of digital evidence gathering. Alternatively or additionally, due to limited resources or other reasons, competition authorities may find outsourcing digital evidence gathering to other public agencies which already developed that capacity more feasible. In such cases, it is good practice to conclude a protocol between the competition authority and the other public agency to describe the scope and nature of co-operation (ICN, 2014, pp. 12-14[1]).

42. Building and maintaining capacity to gather digital evidence during unannounced inspections may put serious pressure on an agencies' financial and human resources. High costs can be the most significant impediment to undertake capacity building actions. Open-source software development and co-operation between competition authorities in terms of training can help to overcome some of the challenges.[17]

4.2. Privileged Information

43. As a corollary to the right of defence and fair trial, some information is treated as privileged from disclosure to third parties, including public authorities, in many jurisdictions. One of these privileges is the confidentiality of communications between a lawyer and its client regarding legal advice. Legal professional privilege is not only an evidentiary rule but it also protects the privileged communications from seizure or review by third parties without the consent of client. (OECD, 2018[12]) In this context, methods of digital inspections such as imaging or copying a digital medium entirely or seizing an unchecked amount of original digital data could infringe legal privilege rules.

44. During physical searches in unannaunced inspections, representatives of the inspected party can easily intervene to claim privilege and consequently avoid copying, seizure and review of the document. This is impossible for data stored on a seized medium or completely copied from servers. Even though privilege may be claimed for a part of the data eventually, privileged information will be temporarily copied or seized.

45. Privileged information can be identified with the use of the same forensic tools that are used for searching the data. This can ensure that the software identifies documents with "privilege" label and all the electronic documents can then be treated the same way as physical documents in order to decide about their legal characteristics. It is also suggested that the inspected party can provide search terms to be run against the indexed data to detect privileged documents (Polley, 2013, p. 22[9]) or names of legal advisors can be excluded from the search terms of the inspection team (Lang, 2014, p. 15[8]).

4.3. Privacy and Data Protection

46. Digital evidence gathering may also infringe privacy rights of the employees of the inspected undertaking and third parties. As it was mentioned above, processing huge amounts of data with digital tools involves the risk including data that are protected under privacy rights. This risk is augmented further by "bring your own device" (BYOD) policies of firms. BYOD policies allow employees to use their personal devices such as smart phones and tablets at the workplace and for work purposes. This may cause difficulties in

identifiying the digital media to target during inspections and, more importantly, in separating private data from business related data.

Box 2. Inspection of Personal Mobile Devices – A Case from Spain

In 2016, the Spanish National Authority for Markets and Competition Council (CNMC) imposed fines on six nougat producers for agreeing to share the market of the main distributors of white label nougat in Spain between 2011 and 2013. In the course of this case, the CNMC conducted an on-the-spot inspection at the premises of Almendra y Miel SA in 2013. Almendra y Miel SA appealed the decision to Audiencia Nacional. One of the grounds for appeal was breach of right to privacy and IT freedom (*libertad informatica*). It was claimed that the CNMC violated the mentioned rights when it collected confidential and private information of its employee, Mr Claudio, which was stored on his mobile phone. It was argued that access to these data, especially recordings of telephone conversations and graphic documents in his mobile phone, was not authorised and the data was not relevant to the CNMC's investigation.

On 18 July 2016, Audiencia Nacional ruled that private documents not related to company activity should be excluded from the investigation. However, a shallow look at collected documents to determine whether they were private or not did not breach the right to privacy. The decision clarified that the Investigation Order did allow the inspectors to access physical and electronic agendas of company employees, including the ones on their mobile phones.

Audiencia Nacional also decided that, despite Mr Claudio's claims of unauthorized seizure of his phone and the review of its content in his absence, the inspection proceeded correctly. In the decision, it is explained that according to inspection minutes, Mr Claudio was present and asked to discard documents which are personal or protected by attorney-client privilege. Once these types of documents were separated, the inspection of the remaining documents (including his phone) was held in another room without the presence of employees of the company. It was emphasised that the company signed the inspection minutes without any protests.

It was also decided that the inspection of telephone conversations which were digitally archived in Mr. Claudio's phone was not a breach of IT freedom. It was concluded that there was no evidence that his personal data was used for purposes other than the legitimate one which justifies its obtaining. It is also highlighted that the disputed documents were not included in the investigation file at the end of the proceedings.

Sources: Decision of Audiencia Nacional dated 18 July 2016, D. Claudio, Almendra y Miel SA y Confectionary Holding SL v CNMC, No 136/2014, ES:AN:2016:2986.
http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7784395&links=&optimize=20160805&publicinterface=true
Employee's mobile phones not safe from dawn raid scrutiny, Spanish court finds, *http://competitionlawblog.kluwercompetitionlaw.com/2016/09/16/employees-mobile-phones-not-safe-from-dawn-raid-scrutiny-spanish-court-finds/*

47. In some jurisdictions, collection and processing of personal data are regulated by data protection rules. Depending on the degree of protection provided by the laws and regulations of the jurisdiction, competition authorities may need to adapt their workflows, procedures and methods of unannounced inspections to data protection regulations. For instance, a competition authority may be obliged to inform the data subject (employee of the inspected undertaking) about her/his rights, the purpose of data processing (e.g. removal of a hard drive or blocking access to a mailbox), and the recipient of the personal data. Another challenge for competition authorities can be rights of data subjects under data protection regulations, such as right to request access to their personal data, obtain rectification or object to its processing (Kuschewsky and Geradin, 2014[13]). However, it is important to underline that data protection rules and principles are not totally alien to competition authorities since the

principles they already adhere to, such as legality, proportionality and security in general contribute immensely to meet the data protection goals.

4.4. Location of the Digital Information

48. In the digital world, data is not necessarily stored at the location where it is accessible. On the contrary, as new services based on the server-client model or cloud computing become prevalent, storage spaces of digital data are no longer in the same location as the access point. In this context, inspection teams often detect and access data that is stored on servers which are located (i) at another premise of the inspected undertaking at a different address, (ii) at the premises of a third party, (iii) outside of the jurisdiction of the competition authority (ICN, 2014, p. 28[1]).

49. Many agencies adopt an access approach. According to this approach, as long as the data is accessed, controlled and used by the undertaking from the inspected location, the data is considered within the reach of digital inspection. In this case, none of the above mentioned locations constitute an obstacle to copying and examination of the data.[18]

50. Alternatively, location approach can be adopted. According to that approach, competition authorities can only search digital data which is located within its jurisdiction or authorisation. If location approach is accepted, a competition agency needs an inspection decision or a court warrant which includes premises of third parties who harbour the servers or the data. In cases where the servers are located outside the jurisdiction's territory, competition authorities have to rely on international co-operation, on *ad hoc* basis or through mutual legal assistance treaties.

51. In this sense, the location approach puts competition authorities in a very challenging situation. First of all, locating the places of servers and other data storage units can be extremely difficult during the planning stage of an inspection. If the location of servers is only found out during an inspection, new legal documents must be issued immediately since digital evidence is in jeopardy until the inspection team can secure the digital data. Furthermore, slow functioning *ad hoc* international cooperation and mutual legal assistance treaties seem unrealistic options as unannounced inspection generally aim to benefit from surprise element and the evidence can be lost in the meantime. What is more, cloud computing stores data in unknown locations on the internet. In such cases, a strict location approach can lead to immunisation of data stored on clouds against inspections.

4.5. Transparency

52. Digital inspections are a relatively new addition to unannounced inspections. Tools and procedures for digital searches are also open to change as technology develops and experience accumulates. Although more and more competition authorities collect and analyse digital data, undertakings do not always know what to expect in these inspections.

53. Transparency generally benefits all the parties of the proceedings. Transparency can be particularly important for competition authorities since it is a crucial component of an efficient and effective investigation. Transparency improves evidence gathering process through encouraging cooperation between the parties and the competition authority and speeding up the process (OECD, 2010, p. 9[14]) (ICN, 2013, p. 4[15]).

54. As regards unannounced inspections of digital data, competition authorities must assess the pros and cons and the intended level of transparency carefully. On the one side,

informing inspected party about what is being searched can facilitate co-operation and ensure that the digital inspection is quick, precise and through. A high level of transparency about the process of digital evidence gathering helps to keep a competition agency's digital evidence gathering procedures consistent and fair.

55. On the other side, competition authorities may be worried that a too precises knowledge of the digital data gathering methods and targets coud jeopardise the success of an unannounced inspection. It could facilitate the destruction of digital evidence or help to block access to it. In terms of procedures, transparency may make the authority less flexibile in digital evidence gathering (ICN, 2014, pp. 30-31[1]). While some competition authorities have already published guidelines that include their approach to digital evidence[19], others may want to reach a certain level of experience and wait for judicial guidance before they publish explanatory materials.

5. Conclusion

56. Digitalisation takes place at great pace. In an environment where almost all information is produced, processed or stored digitally, unannounced inspections cannot be effective without digital evidence gathering.

57. There are some principles based on evidence law and forensics discipline regarding digital inspections. These principles can be grouped under four headings: legality, competence, integrity and security, and authenticity. Authorities must establish their procedures and methods in the light of these principles.

58. Digital evidence gathering practices of competition authorities vary. As it is a relatively new practice there is not sufficient precedent or experience yet to answer all the potential questions. Also the practice of digital inspections vary widely among the jurisdictions. Some challenges are, however, common to all competition authorities: finding the appropriate legal basis of digital evidence gathering, capacity building, proportionality in digital searches, protection of privileged and private data, access to information which is stored outside the jurisdiction of the agency and the question of transparency.

Endnotes

[1] https://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

[2] https://www.radicati.com/wp/wp-content/uploads/2017/12/Email-Statistics-Report-2018-2022-Executive-Summary.pdf

[3] https://www.radicati.com/wp/wp-content/uploads/2015/02/Instant-Messaging-Market-2014-2018-Executive-Summary.pdf

[4] https://www.radicati.com/wp/wp-content/uploads/2017/12/Instant-Messaging-Statistics-Report-2018-2022-Executive-Summary.pdf

[5] See OECD (2013[16]) for an overview of unannounced inspections.

[6] Presentation by UK CMA at OECD Workshop on cartel screening in the digital era on 30 January 2018, https://www.slideshare.net/OECD-DAF/cartel-screening-in-the-digital-era-uk-competition-markets-authority-january-2018-oecd-workshop.

[7] Chain of evidence is record of seizure, analysis and other processing of the digital evidence which proves the evidence is extracted from the seized digital information without doubt (ICN, 2014, p. 5[1]).

[8] Chain of custody is the record of custodial history of the digital evidence which proves its provenance (ICN, 2014, p. 5[1]).

[9] "Live forensics consists of seizing or analysisng system information, memory contents and/or contents of data cariers from live systems (*i.e.* systems that are on/running). This extracts information from live memory (*i.e.* information which is lost when the computer devices or systems are turned off/powered down)." (ICN, 2014, p. 6[1])

[10] A hash value is a unique numeric value that identifies data like a digital finger print. It is produced by mathematical algoritms. Data cannot be changed without changing the corresponding hash value. (ICN, 2014, p. 6[1])

[11] Stand-alone judicial review may have some drawbacks too such as lacking enhanced precision of retrospective review and prolonging total duration of the proceedings (Simonsson, 2013, p. 13[11]).

[12] Decision of the Court of Justice of the European Union, Deutsche Bahn AG and Others v European Commission, 583/13, EU:C:2015:404, para. 61-68, http://curia.europa.eu/juris/document/document.jsf?text=&docid=165109&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1238484

[13] Decision of the Court of Justice of the European Union, Dow Benelux v Commission, 85/87, EU:C:1989:379, para. 19, https://eur-lex.europa.eu/resource.html?uri=cellar:ac7eff8a-c8af-4815-8653-62d0d4662c69.0002.03/DOC_2&format=PDF

[14] Anti-Cartel Enforcement Template – Hungary, p.21, http://www.gvh.hu/data/cms1032890/HUN_Cartel_Template_with_settlement_2016_02_01_final.pdf

[15] Press release of Hungarian Competition Authority, http://www.gvh.hu/en/press_room/press_releases/press_releases_2007/4853_en_gvhs_winning_the_motorway_cartel_case_became_final.html

[16] According to Swedish Competition Law, KKV can take digital data to its premises to examine it only on the condition of inspected party's consent.

[17] According to ICN (2014, p. 14[1]), it is advisable to have a dedicated annual budget and multi-annual financial planning for purchase and maintenance of equipment, software and training of staff.

[18] See Polley (2013[9]) for critique of the access approach.

[19] For instance, the Netherlands Authority for Consumers and Markets published "AMC Procedure for the inspection of digital data" in 2003 and undated in 2014. https://www.acm.nl/sites/default/files/old_publication/publicaties/12772_2014-acm-procedure-for-the-inspection-of-digital-data-2014-02-06.pdf

The EU published "Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003" that also provides guidance on digital inspections http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf

Austrian Federal Competition Authority published "Guidance on dawnraids" which includes a section on "Collection of electronic data" https://www.bwb.gv.at/fileadmin/user_upload/Downloads/standpunkte/Guidance_on_dawn_raids_final.pdf

References

APCO (2012), *ACPO Good Practice Guide for Digital Evidence*, https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. [3]

ECN (2013), *ECN Recommendation on the Power to Collect Digital Evidence, Including by Forensic Means*, http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf . [4]

ECN (2012), *Investigative Powers Report*, http://ec.europa.eu/competition/ecn/investigative_powers_report_en.pdf. [6]

ICN (2014), *Chapter on Digital Evidence Gathering*, http://www.internationalcompetitionnetwork.org/uploads/library/doc1006.pdf. [1]

ICN (2013), *Competition Agency Transparency Practices*, http://internationalcompetitionnetwork.org/uploads/library/doc902.pdf. [15]

Jalabert-Doury, N. (2009), "Digital evidence searches in competition investigations: Best Practices for effective fundametal rights", *Concurrences*, Vol. 4, https://www.concurrences.com/en/review/issues/no-4-2009/articles/Digital-evidence-searches-in-29118. [10]

Tanel Kerikmä, A. (ed.) (2016), *Challenges in Collecting Digital Evidence: A Legal Perspective*, Springer. [5]

Kuschewsky, M. and D. Geradin (2014), "Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges", *World Competition*, Vol. 37/1, pp. 69-102, https://www.kluwerlawonline.com/abstract.php?area=Journals&id=WOCO2014005. [13]

Lang, J. (2014), "Legal problems of digital evidence", *Journal of Antitrust Enforcement*, Vol. 2/1, pp. 1-25, https://doi.org/10.1093/jaenfo/jnt007. [8]

Michalek, M. (2015), *Right to Defence in EU Competition Law: The case of Inspections*, University of Warsaw Faculty of Management Press. [7]

OECD (2018), *Treatment of Legally Privileged Information in Compeititon Proceedings*. [12]

OECD (2013), *Unannounced Inspections in Antirtust Investigations*, https://one.oecd.org/document/DAF/COMP/LACF(2013)6/en/pdf. [16]

OECD (2010), *Procedural Fairness: Transparency Issues in Civil and Administrative Enforcement Proceedings*, http://www.oecd.org/daf/competition/mergers/48825133.pdf. [14]

Polley, R. (2013), *Digital Evidence Gathering in Dawn Raids - a Risk for the Compay's Rights of Defence and Fundamental Rights*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2355033. [9]

Simonsson, I. (2013), *Digital Evidence Gathering in Dawn raids. Judicial Review: Up-Front or Retrospective*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327122. [11]

US DoJ (2004), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf. [2]