Organisation for Economic Co-operation and Development

DAF/COMP/LACF(2020)14

Unclassified

English - Or. English

8 September 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

LATIN AMERICAN AND CARIBBEAN COMPETITION FORUM - Session I: Digital Evidence Gathering in Cartel Investigations

- Contribution from the United States -

28-29 September 2020, virtual Zoom meeting

The attached document from the United States is circulated to the Latin American and Caribbean Competition Forum FOR DISCUSSION under Session I at its forthcoming meeting to be held on 28-28 September 2020, via a virtual Zoom meeting.

Ms. Lynn Robertson, Manager Africa/MENA, LACCF ; Competition Expert - Lynn.Robertson@oecd.org.

JT03465050

Session 1: Digital Evidence Gathering in Cartel Investigations

Legal and Practical Challenges of Digital Evidence Gathering

- Contribution from the United States -

1. The digitalization of the global economy has challenged competition enforcers around the world to modernize the way they investigate cartels and adapt to the new ways that companies use technology to do business. Digitalization has also revolutionized the way that people communicate with one another, and has raised important questions about individual privacy and liberties for targets of a cartel investigation. This submission will outline some of the legal and practical considerations for the Department of Justice Antitrust Division ("Division") in digital evidence gathering in cartel investigations. The first section discusses the legal framework for obtaining evidence from companies that provide electronic communication services. The next section describes the work of the Division's specialized litigation support team. The final section concludes with a discussion of the legal framework for conducting seizures of evidence and practical challenges with seizing digital evidence.

1. Obtaining Digital Evidence from Third-Party Electronic Communication Providers

2. Cartelists have adapted to the digital world. Conspirator conversations in "smoke-filled back rooms" have now moved to email and beyond, including encrypted messaging applications. In many cases cartelists, conscious of the illegality of their activity, have switched from their corporate email accounts to personal email and messaging services provided by third parties, such as Google's Gmail or Facebook Messenger, to communicate with co-conspirators. As conspirators have become smarter about the way they communicate with each other, the Division has adapted its investigative techniques, and now frequently seeks to obtain digital evidence from third-party communications companies during the course of a cartel investigation.

3. In the United States, Title II of the Electronic Communications Privacy Act ("ECPA") governs how and when any U.S. law enforcement agency, including the Division, can obtain access to stored digital communications, such as email or phone records, during the course of a criminal investigation.[1] ECPA is designed to provide U.S. law enforcement agencies with tools to effectively prosecute crime, while also providing privacy for individuals and ensuring protection from unreasonable searches and seizures, a concept enshrined in the 4th amendment of the U.S. Constitution. The law applies to providers of electronic communication services or remote computing services who supply those services to the general public. These include web and app-based email and messaging providers, social media companies, and companies that provide computer storage or processing services such as cloud services, webhosting, or online photo storage.

[1] *See* 18 U.S.C. §§ 2701–2713.

4. ECPA has several key features that are relevant to conducting criminal cartel investigations, which will be discussed in further detail below:

- ECPA distinguishes between the "content" of a communication and other records or information that do not contain content;
- ECPA requires companies to preserve data upon the request of a U.S. law enforcement agency;
- ECPA allows U.S. law enforcement agencies to obtain a court order requiring a company not to disclose receipt of an order, subpoena, or search warrant to the customer for a certain period of time; and,
- A recent amendment to ECPA, the CLOUD Act, requires providers operating within the U.S. to produce evidence regardless of whether the company stores the evidence in the U.S.

5. *Content vs. Non-Content Data.* A key feature of the law is the distinction between the "content" of communications, and other records or information relating to the account, including customer identification information and transactional records that are not considered "content." Information defined as "content" is subject to a higher level of privacy protection. In most cases, prosecutors will obtain a search warrant for any "content" information, which requires judicial approval and a showing of probable cause that the content of a communication contains evidence of a crime. "Content," for example, includes the body of an email message, or the text of an SMS message on a phone.

6. Information that is not considered to be the contents of a communication, on the other hand, does not have the same level of protection. For example, information about a customer and their account, such as the customer's name and address and their payment information does not require the same evidentiary showing that would be required to obtain the contents of their emails.

7. Non-content information such as subscriber information and transactional records can be particularly helpful in cartel cases to establish contacts between cartel members, even though the content of the communication is not known. For example, email message headers may not show what the targets were discussing, but it will show whether suspected cartel members were communicating with each other and when. Activity logs indicating when suspected cartel members have accessed their accounts or submitted bids could indicate that the individuals were working together in coordination.

8. *Data preservation*. Communications providers are required to preserve records upon the request of a U.S. law enforcement agency, initially for a 90-day period that can be renewed once.[2] This is useful in case the subjects of an investigation delete messages from their phones or email accounts; the messages can then be obtained directly from the provider using a warrant or other appropriate process under ECPA.

9. *Confidentiality*. Importantly, the Division can obtain a court order preventing a provider from disclosing to their customer that the company has received a warrant, court order, or subpoena for information relating to their account.[3] When evaluating a request for a non-disclosure order, the court determines whether disclosure will result in destruction of evidence, seriously jeopardize the investigation, or unduly delay a trial, among other

[2] *See id.* § 2703f.

[3] *See id.* § 2705b.

things.[4] This non-disclosure order can last for a period of time determined by the court to be "appropriate."[5] Under current Department of Justice ("DOJ") policy, prosecutors may only seek orders lasting for one year or less.[6]

10. *Location of evidence*. In 2018, the U.S. Congress enacted the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which amended ECPA to make clear that a company subject to jurisdiction in the U.S. must produce data that it controls, regardless of whether the data is stored on U.S. soil.[7] This legislation was, in part, a result of a case involving Microsoft's refusal to comply with a search warrant because the data was stored on an overseas server. In 2013, Microsoft challenged a search warrant issued under ECPA by a U.S. magistrate judge.[8] The warrant called for account information and emails of a subject in a drug trafficking investigation. Though a U.S.-based company, Microsoft contended the emails were stored on a server in Ireland, and thus, not subject to the jurisdiction of U.S. courts. The challenge was ultimately appealed to the Supreme Court, but the case was vacated when Congress passed the CLOUD Act.[9] As a result, it is now clear that all providers of electronic communications subject to ECPA are required to produce evidence within their "possession, custody, or control" regardless of whether the data is stored in the U.S. or at another location overseas.

11. *Practical challenges*. Obtaining digital evidence through ECPA can provide both direct, "smoking-gun" evidence of a cartel conspiracy as well as circumstantial evidence that shows conspirators engaged in actions consistent with an agreement or efforts to conceal the conduct, indicating consciousness of guilt. As with anything, there are practical challenges to using this type of evidence effectively. The sheer volume of material produced can be burdensome and costly to process and review. The Division is also confronting new types of document formats, such as image-based services that allow users to communicate through sharing photos, gifs, emojis, stickers, and the like. Processing these digital materials and packaging them in a reviewable format for agency staff is a new challenge for competition agencies. DOJ's approach to handling the practical challenges of digital evidence is discussed further below.

2. Managing Digital Evidence

12. The Division has a specialized litigation support team that facilitates the gathering, processing, and reviewing of digital evidence in all Division cases, including criminal cartel cases. Our litigation support team is made up of professionals with education and experience in the fields of information technology ("IT"), legal case management, and project management, with a particular emphasis on experience with litigation, eDiscovery, and forensic tools.

---

[4] *Id.* (the provision includes a list of five factors).

[5] *Id.*

[6] U.S. Dep't of Just., Just. Manual § 9-13.700, https://www.justice.gov/jm/jm-9-13000-obtaining-evidence#9-13.700.

[7] *See* 18 U.S.C. § 2713.

[8] *In re Warrant To Search a Certain E-Mail Acct. Controlled and Maintained by Microsoft Corp.*, 15 F.Supp.3d 466 (S.D.N.Y. 2014); *See also In re Warrant To Search a Certain E-Mail Acct. Controlled and Maintained by Microsoft Corp.*, 829 F. 3d 197, 204–205 (2d Circ. 2016).

[9] *U.S. v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

13. In the Division's experience, communication and coordination between the Division IT staff and investigative teams is vital to ensuring efficient receipt and processing of digital evidence. Staff must be trained to effectively use the technology tools to review that evidence. Every Division investigation is assigned a Case Manager from the litigation support team who is part of the investigative team from the beginning of the case to the resolution, including at trial. The Case Manager is there to provide guidance on a range of issues related to production of digital evidence and helps manage the processing of digital evidence for review, including both seized evidence and evidence produced in response to a subpoena or voluntary request.

14. The Division's litigation support team also includes personnel with specialized technical expertise that consult with investigative teams across the Division on a variety of topics such as using database review platforms, document imaging and coding, production of forensic acquisitions, and trial presentation software.

15. Another important function of the litigation support team is advising on developing and implementing protocols for investigative teams to follow related to the production, processing, and review of evidence. The litigation support team also provides training to legal and economic staff on how to use the various technology tools that the Division employs, including database review platforms.

16. In addition to the litigation support team, the Division's Senior Counsel for Electronic Discovery acts as a liaison between the litigation support team and our legal and economic staff, and leads the development and implementation of best practices and guidance on subjects ranging from using search terms to preserving documents and negotiating production of digital evidence. Our Senior Counsel for Electronic Discovery also leads a working group on electronic discovery, made up of staff from across the Division. To specifically tackle the increasing challenges in cartel cases, the Division recently hired a specialized trial attorney who focuses on electronic discovery in criminal cartel cases. She is assigned to some of the Division's most complex cases, and provides expertise and guidance on issues arising with digital evidence throughout the lifecycle of an investigation.

3. Seized Digital Evidence – Obtaining Evidence Directly from the Subjects

3.1. Legal and Practical Considerations

17. *Legal Process for Seizures*. One tool widely used by competition agencies for detection and prosecution of hardcore cartels is the unannounced inspection, or "dawn raid," conducted at both businesses and private premises. In the United States, the Division's version of a "dawn raid" is the execution of a search pursuant to a warrant. Under U.S. law, the Fourth Amendment to the U.S. Constitution protects individuals from unreasonable searches and seizures, and establishes the basic requirements for warrants issued for searches and seizures; Rule 41 of the Federal Rules of Criminal Procedure further explains the process for obtaining and executing a search warrant.[10] Conducting an unannounced inspection in a criminal antitrust case is done pursuant to a Rule 41 search warrant issued by an impartial judicial officer, generally a federal magistrate judge, upon a showing that there is probable cause to believe that a crime has been committed and that

[10] U.S. Const. amend IV; Fed. R. Crim. P. 41. There are several very limited exceptions to the requirement for a warrant, including consent, a search performed incident to a lawful arrest, and the plain view doctrine.

evidence of the crime is likely to be found in the particular location specified in the warrant.[11]

18. To obtain a warrant, a U.S. law enforcement officer must provide a sworn affidavit that alleges the facts establishing probable cause and describes the location to be searched and items to be seized. For Division prosecutors, it is important to ensure that searches and seizures are conducted in accordance with the law and the procedural protections afforded by the Fourth Amendment, to avoid potential suppression of the evidence later by the court during a trial. The Division works closely with our federal law enforcement partners in both preparing search warrants and planning their execution.

19. Searches pursuant to a warrant are a key investigative tool utilized by the Division. Searches create a heightened fear of detection that destabilizes cartels and incentivizes self-reporting.[12] The Division Manual also addresses the importance of searches in obtaining evidence of hardcore cartels, highlighting that the use of searches "minimizes the opportunity for document destruction and concealment, prevents the failure to produce responsive documents either deliberately or through inadvertence, and often spurs a race for leniency."[13]

20. Conducting a search of a corporation or private premise regularly involves seizing digital evidence that may be stored on a device or on a server. Corporate computers, servers, and smartphones may contain evidence of a cartel, but may also contain other documents and information that are unrelated to our investigation. It is generally impractical to do a file by file review of electronic evidence to determine what documents are truly relevant during the onsite search operation. Where such review is impractical, Rule 41(e)(2)(B) creates a two-step process for seizures of digital evidence. Digital media is seized or copied onsite during the execution of search warrant, then later reviewed to determine which contents fall within the scope of the warrant.[14]

21. *Legal Privilege & Seized Evidence*. One key legal consideration in seizing digital evidence in a cartel investigation is the protection of attorney-client privilege. Seizures of corporate evidence in a cartel case may involve seizing digital communications with both in-house and external lawyers, and some of those communications may be privileged. The attorney-client privilege is a long-standing privilege recognized in U.S. law that protects communications between an attorney and his client. It can be asserted in response to legal demands for discovery and other compelled disclosures, including testimony. It applies in both civil and criminal matters, and can attach for private individuals, corporations, and even governmental clients.

22. Like many common law doctrines, the attorney-client privilege has certain essential elements. The person asserting the privilege must be a client and the communication must be with a licensed attorney. Attorneys are broadly defined to include in-house counsel, government lawyers, private lawyers, and those they hire to assist them (experts, paralegals, and support staff). However, not every communication with a lawyer will be privileged. The communication must relate to legal advice; if a corporate lawyer is giving business advice to their company, that would not be a privileged communication. And there are

[11] *See id.*

[12] *See e.g.,* U.S. Dep't. of Just., Richard A. Powers, Deputy Assistant Att'y Gen., *A Matter of Trust: Enduring Leniency Lessons for the Future of Cartel Enf't* (San Francisco, CA, February 19, 2020), https://www.justice.gov/atr/page/file/1250346/download.

[13] *See* U.S. Dep't. of Just., Antitrust Div. Manual § III-90.

[14] *See* Fed. R. Crim. P. 41(e)(2)(b).

exceptions, including the "crime-fraud" exception, for situations in which a lawyer may be involved in the crime or may be providing advice about how to commit the crime, such as advising a corporate client on how to engage in price fixing.[15]

23. In practice, the protection of attorney-client privilege means that if we have reason to believe any seized materials include potentially privileged documents, the Division will take steps to remove those documents from the collection of seized material before the investigative team can review. This can be done in a number of ways. The Division may conduct its own review for potentially privileged documents using a team of attorneys that are independent from the investigative team, sometimes referred to as a "filter team." The filter team will segregate any potentially privileged materials, and then provide the investigative team access to the remaining materials that do not include potentially privileged materials. In the alternative, the review for privileged materials may be done by the company or individual's attorney following the seizure and before the investigative team reviews the seized materials. The investigative team would only review the materials deemed not privileged by the company or individual's attorney.

24. Legal privilege is also an important consideration in the international context. The globalization of cartel enforcement raises questions about how to address attorney-client privilege, and presents difficult issues of bridging civil and common law traditions. Many civil law jurisdictions that do not recognize attorney-client privilege have enacted statutory confidentiality rules that obligate attorneys not to disclose confidential information the client provided to the attorney. However, this often applies only to the attorney, not the client, and may only include outside counsel. As a result, a dawn raid of the client's offices, or a document request targeting the client but not the lawyer, may not provide any protection to a client's confidential information. And while this approach was workable in an age when clients visited their attorney's offices to secure advice and exchange information, in a world of digital communication and global business, this is a fundamental gap in privilege protections. The Division supports working toward common practices on attorney-client privilege to promote core due process standards.[16]

25. *Forensics and Encryption*. When seizing digital evidence, it is important to remember that computers and other devices are not simply made up of files, folders, and applications that are accessed by the user. A forensic examination of a device will reveal metadata and other artifacts that may provide useful information about how a device has been used, when files have been accessed and modified, internet search history, attachment of USB storage devices, and other traces of information that indicate how an individual used the device. This type of forensic information can be useful to show knowledge or intent, to corroborate witness statements, and to counteract defendants' claims that they had no knowledge or control over particular documents or shared network spaces. Importantly, a forensic search may also reveal information in a computer's memory that can assist an agency with decrypting an encrypted device. These types of forensic examinations can be time consuming and need to be conducted in concert with certified forensic examiners specially trained on the handling of forensically acquired data.

[15] *Clark v. United States*, 289 U.S. 1, 15 (1933) ("The privilege takes flight if the relation is abused. A client who consults an attorney for advice that will serve him in the commission of a fraud will have no help from the law.").

[16] *See* U.S. Dep't. of Just., Roger Alford, Deputy Assistant Att'y Gen., *Remarks at the Nat'l Autonomous Univ. of Mexico (UNAM) Event Sponsored by the Fed. Comm'n of Econ. Competition (COFECE)* (Mexico City, MX, May 30, 2018), https://www.justice.gov/opa/speech/file/1066916/download.

26. *The importance of pre-seizure planning*. Executing a search that will involve seizure of digital evidence requires careful consideration of the legal issues discussed above. Searches also present numerous practical challenges. Reviewing seized devices or forensic images of digital media to determine what falls within the scope of the warrant and what materials may be privileged takes time. A large volume of digital evidence takes time to process and load into a review database. In the Division's experience, the key to successfully addressing these legal and practical challenges is pre-seizure planning and communication between the legal staff leading the case, the law enforcement agency executing the search, and the Division's litigation support staff. In these pre-seizure planning conversations, the Division legal and litigation support staff and the seizing agency can work together to, among other things, devise more targeted search strategies that will result in a smaller volume of materials to process, discuss timing of searches and organization of materials, develop a system for tracking and logging seized items, and design a plan to handle privileged materials.

4. Conclusion

27. While this paper lays out some of the basic legal regimes in the U.S. that govern the collection of digital evidence, it is important to note that this area of the law is constantly evolving. As technology advances apace and the way in which people interact with and use technology in their daily lives continues to change, there will continue to be challenges to the laws and legal precedents governing how and when U.S. law enforcement agencies can obtain a person's emails, text messages, or other digital communications. The Division has criminal prosecutors designated as specialists in computer crimes, and they monitor changes in this area of the law and provide training, guidance, and support to other attorneys and staff. As mentioned above, the Division also has dedicated litigation support staff who work to adapt Division practices to new developments in technology and the law. As competition agencies across the globe work to adapt to these new challenges, the Division looks forward to sharing experiences with and learning from our international partners.