International Antitrust Bulletin

ABA SECTION OF ANTITRUST LAW
Promoting Competition Protecting Consumers

ABA Section of Antitrust Law | International Committee | August 2014 | Vol. 2

Contribute to the IAB

If you have a topic idea, please contact one of our Editors-in-Chief, Tom Collin or Krisztian Katona. Articles can cover any topic in the international antitrust area and should be approximately 800-1,200 words.

Join the International Committee

If you'd like to join our Committee, please visit www.ambar.org/atInternational.

Follow us on:

The International Antitrust Bulletin is published four times a year by the American Bar Association Section of Antitrust Law International Committee. The views expressed in the International Antitrust Bulletin are the authors' only and not necessarily those of the American Bar Association, the Section of Antitrust Law or the International Committee. If you wish to comment on the contents of the International Antitrust Bulletin, please write to the American Bar Association, Section of Antitrust Law, 321 North Clark Street, Chicago, IL 60654-7598.

IN THIS ISSUE

What In The World Did I Miss?

A summary of the world's major competition law developments in the past quarter.

North America

South America

Asia

Europe

New Guidance on the Collection and Seizure of Electronic Evidence in International Cartel Cases

Mark Krotoski[1]
U.S. Department of Justice, Antitrust Division, United States

In April 2014, the International Competition Network (ICN) Cartels Working Group released new, updated chapter on "Digital Evidence Gathering" for international antitrust enforcement.[2] The primary objectives of the chapter are to explain "ICN member approaches to digital evidence gathering and to identify good practices and procedures" for the collection and seizure of this evidence during the investigation and prosecution.[3]

The update provides useful suggestions concerning the preservation, identification, and seizure of electronic evidence in cartel cases. The recommendations may also aid leniency applicants since electronic evidence is regularly provided to competition agencies in the leniency process. This article highlights some of the best practices noted in the new guidance and the increasing importance of electronic evidence in international cartel enforcement.

Growing Role of Electronic Evidence in Cartel Enforcement Cases

The amount of electronic data created and used by business continues to grow exponentially. A recent report estimates that in 2014 more than 108 billion emails were sent and received by businesses *each day*. Daily business email use is expected to increase in 2018 to nearly 140 billion.[4] As part of this digital trend, some businesses now promote paperless practices. Consequently, some records will be created and exist only in electronic form.

Not surprisingly, electronic evidence can provide numerous benefits in a cartel investigation and prosecution. Illustratively, key cartel electronic records, such as "competitive strategy and communication between" competitors, may be located in an examination of seized data.[5] Emails between cartelists have highlighted how collusion was planned and executed.[6] Electronic communications may confirm meeting locations, including those in other countries. Electronic records provide metadata (or data about data) concerning the history of the records.[7] By using "hash values," also known as "digital fingerprints" or "digital DNA," examiners can determine how many records exist for a particular document.[8] "User attribution" information can be used to identify the author of a particular record.[9] Deleted electronic records may be recoverable.[10] Electronic records can be used to corroborate other key evidence in the investigation and to provide new leads for investigators.

However, there are a host of challenges in identifying, preserving, collecting and analyzing electronic evidence in a cartel investigation. Consider a couple of examples. Company data may be stored in multiple locations, including on the network, external servers, storage media (such as hard drives and thumb drives), cell phones, and in the cloud.[11] Further, some of the data may be stored in different jurisdictions and countries. In these circumstances, coordination among competition agencies is necessary to maximize the opportunity to seize relevant evidence and minimize the risk of destruction of records in multiple locations. Electronic records can be fragile, based on limited retention periods by Internet providers or company policies. Efforts may be taken to destroy electronic records, presenting forensic challenges in recovering the records. Electronic records may be maintained in multiple languages, requiring translation services to identify and understand key evidence. Data may be encrypted and require company assistance to obtain encryption keys or the use of decryption tools[12]

Managing the Collection of Voluminous Amounts of Data

As the new chapter notes, competition agencies seize or obtain electronic evidence through three primary avenues: (1) searches, raids and inspections; (2) compelled production; and (3) through a leniency application.[13] Electronic evidence is now common for each manner of collection.

Given the voluminous amount of data that may be obtained in a cartel investigation, the ability to manage the collection effectively and efficiently by competition agencies remains essential. There are tradeoffs. One central challenge is to identify and seize relevant information concerning the cartel investigation. At the same time, investigators seek to avoid the over collection of data. Also, the relevance of some key terms and data may not be known until later in the investigation.

Early "Electronic Evidence Case Plan"

In addressing the challenges in managing collection of data, one key best practice concerns the early development of an Electronic Evidence Case Plan ("Plan"). The Plan promotes efficiencies by identifying likely electronic evidence and preserving it for seizure. The new chapter suggests that competition agencies consider establishing a Plan early in a case for identification, preservation, and collection of digital evidence. The Plan will focus on such matters as what types of digital evidence may be used, where it is located or stored, and in how many places it may be found. These matters will affect the timing of any search, raid or inspection and maximize the seizure of digital evidence.

It is usually not possible to collect all of the electronic evidence involved in the case. For example, some evidence may be in multiple locations beyond the reach of enforcers. A Plan will enhance the likelihood that relevant evidence is identified and collected. It may include some of the following issues and factors:

- How was the offense committed? For example, what computers and devices may have been used?
- What type of electronic records were created and maintained?
- Where is the electronic evidence stored and located for collection?
- In how many places can the same or similar evidence be found?
- What retention policies or timing issues may affect collection of electronic evidence? What preservation authority may be used to preserve the evidence pending legal process (discussed below)?
- What legal process may be necessary to obtain electronic evidence (such as search warrant, Mutual Legal Assistance Treaty request)?
- Are there any unique circumstances that should be considered in the case?

Contrasting Electronic and Hard Copy Evidence

Notwithstanding the increasing number of electronic records created by businesses, an effective investigative strategy should focus on capture of *both* electronic and hard copy versions. In fact, both forms of evidence may highlight distinct evidentiary leads or information.[14] A hard copy may contain fingerprints, hand writing or other special notations. The same record in electronic form will not have these features but may include metadata that reveal multiple drafts, authorship, and other historical information.

While there may be only one or a few hard copies, the electronic records may be stored and found in multiple locations. For example, an email that is sent from cartelist A to cartelist B may be found on the sender's device or computer, the Internet Service Provider server, company servers, the recipient's Internet Service Provider server, and the recipient's device or computer, among other locations. Relevant records may be found anywhere along the path of transmission of a communication. Investigators should seek to find all versions of a record.

Taking Necessary Steps to Preserve Electronic Evidence

As already noted, preservation is a key aspect of any Plan. The ICN chapter highlights the importance of "[p]reserve[ing] digital information before any search begins to avoid destruction or alteration."[15]

Some jurisdictions permit law enforcement agencies to preserve data pending sufficient legal process. For example, in the United States, law enforcement officials may request that an Internet Service Provider preserve email or other account information pending appropriate legal process, such as a search warrant.[16] The preservation lasts for 90 days and can be extended an additional 90 days. No information is obtained until legal process has issued. The preservation request ensures that the data are available once legal process has issued.

On the international level, the ICN chapter notes that "the G8 24/7 Network provides an avenue to request the preservation of electronic evidence in other countries pending legal process."[17] This network supplies the most effective means for competition agencies to preserve electronic evidence in other foreign jurisdictions once program requirements are met.

Obstruction of Justice

The ICN chapter also notes the importance of employing "digital evidence gathering practices and procedures that inhibit and help prevent destruction of digital evidence and obstruction."[18] As recent investigations have highlighted, it is not uncommon for records to be destroyed as soon as information is obtained about the investigation or even during or after a dawn raid. By using forensic tools, enforcers have been successful in restoring or recovering data deleted during or after an investigation.[19]

Competition agencies have demonstrated the ability to hold executives accountable for obstruction of justice involving the destruction of electronic records in other jurisdictions. In one recent case, an executive of an international company learned that the FBI was executing a search warrant at company offices in the United States concerning potential violations of antitrust laws. In another country he began deleting numerous emails and electronic files which "contained communications between" his company "and one or more of its competitors regarding Requests for Quotation made by" a manufacturer. Later, in court papers, he admitted that he "deleted these e-mails and electronic files with the intent to impair the availability of these e-mails and electronic files for use in the government's investigation."[20] In March 2014, the executive pled guilty to obstruction of justice in the United States and was sentenced to serve one year and one day in federal prison.

Conclusion

The ability to obtain relevant electronic evidence is increasingly important in cartel investigations. The recently issued ICN chapter on Digital Evidence Gathering identifies several useful best practices for the collection and use of electronic evidence in cartel enforcement. Early creation of a Plan remains central to identifying, preserving, and collecting relevant evidence in an effective and efficient manner. In the end, each cartel case requires a tailored forensics approach to see that the particular needs and issues of the investigation are addressed.

---

[1] The views in this article do not necessarily reflect those of the Department of Justice.

[2] Cartel Enforcement Subgroup 2: ICN Cartels Working Group, Anti-Cartel Enforcement Manual Chapter on Digital Evidence Gathering (hereinafter "Digital Evidence Gathering Chapter"), *available at* www.icnmarrakech2014.ma/pdf/Anti-Cartel_Enforcement_Manual.pdf. The chapter updates a prior one from March 2010. *See* Anti-Cartel Enforcement Manual Cartel Working Group, Subgroup 2: Enforcement Techniques, Digital Evidence Gather (March 2010) (Chapter 3), *available at* www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf.

[3] Digital Evidence Gathering Chapter, at 4.

[4] Email Statistics Report, 2014–2018, The Radicati Group, Inc. (April 2014), *available at* www.radicati.com/wp/wp-content/uploads/2014/04/Email-Statistics-Report-2014-2018-Executive-Summary.pdf; *see also id.* at 2 ("Email remains the most pervasive form of communication in the business world, while other technologies such as social networking, instant messaging (IM), mobile IM, and others are also taking hold, email remains the most ubiquitous form of business communication.").

[5] Digital Evidence Gathering Chapter, at 32 (in noting some of the advantages in collecting electronic evidence, "[o]ne competition agency reported that the main advantage is that information about the company's competitive strategy and communication between the competitors are usually found on digital media.").

[6] *See, e.g.*, Antitrust: Commission imposes € 169 million fine on freight forwarders for operating four price fixing cartels (March 28, 2012) (noting "a specific yahoo email account was set up to facilitate exchanges between the cartel participants"), *available at* http://europa.eu/rapid/press-release_IP-12-314_en.htm; *see also* Antitrust: Commission fines producers of high voltage power cables € 302 million for operating a cartel (April 2, 2014) ("The cartelists regularly met each other in hotels in South-East Asia and Europe and maintained further contacts by means of e-mails, faxes and telephone calls."), *available at* http://europa.eu/rapid/press-release_IP-14-358_en.htm.

[7] Digital Evidence Gathering Chapter, at 6 (defining "metadata" as "information about a particular data set or digital document, which describes how, when, and by whom the data set or digital document was collected, created, accessed, or modified.").

[8] *Id.* at 6 (defining hash value as "a mathematical algorithm produced against digital information (e.g. a file, a physical disk, a logical disk) thereby creating a 'digital fingerprint' or 'digital DNA' for that information."). For more on the role of hash values, *see* Carroll and Krotoski, Using "Digital Fingerprints" (or Hash Values) for Investigations and Cases Involving Electronic Evidence, 62 United States Attorneys' Bulletin 44-82 (May 2014), *available at* www.justice.gov/usao/eousa/foia_reading_room/usab6203.pdf.

[9] Digital Evidence Gathering Chapter, at 23, 24, 34 (noting the importance of user attribution evidence).

[10] *Id.* at 32 (in noting some of the advantages in collecting electronic evidence, "[o]ne competition agency reported that the main advantage with making forensic images is the possibility to restore erased data."). "Generally, until data is overwritten it may be recoverable." *Id.* at 5.

[11] *Id.* at 5 (defining "Cloud computing" as "a new supplement, consumption and delivery model for IT services based on the Internet, and typically involves the provision of dynamically scalable and often virtualised resources as a service over the Internet. This comprises common business applications online which are accessed from a web browser, while the software and data are stored on servers in unknown locations on the Internet.").

[12] *Id.* at 6 ("Encryption is the conversion of plaintext to ciphertext through the use of a cryptographic algorithm.").

[13] *Id.* at 10.

[14] *Id.* at 7-8 (contrasting the evidence that may be available from electronic and hard copy formats).

[15] *Id.* at 19.

[16] 18 U.S.C. § 2703(f). For more information on the preservation authority under Section 2703(f), see Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, at 139-40 (2009), *available at* www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; Ryan and Krotoski, Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act, 47 U.S.F. L. Rev. 291, 306-09 (Fall 2012) (providing case examples in which key evidence was preserved under § 2703(f) and examples where cases had to be closed due to the inability to preserve evidence), *available at* www.usfca.edu/uploadedFiles/Destinations/School_of_Law/Academics/Co-Curricular_Programs/(5)SAN47-2RyanandKrotoski.pdf.

[17] Digital Evidence Gathering Chapter, at 19 (providing internet links to further information about the 24/7 Network) (footnote omitted).

[18] *Id.* at 22.

[19] *Id.* at 7 ("Although using digital evidence gathering to locate evidence does not prevent the possibility of obstruction of an investigation, it does provide the possibility of recovering deleted or destroyed evidence.").

[20] *United States v. Kazuaki Fujitani*, Plea Agreement, No. 14-CR-20087-GCS-PJK (EDMI March 11, 2014), *available at* www.justice.gov/atr/cases/f304400/304403.pdf; *see also* Former Denso Corp. Executive Agrees to Plead Guilty to Obstructing Automotive Parts Investigation, Press Release, U.S. Department of Justice (Feb. 20, 2014), *available at* www.justice.gov/opa/pr/2014/February/14-at-177.html.

Meet the Authors

Sabrina Camand is a Junior Associate in the Paris office of Paul Hastings LLP and a member of the Paris Bar. She graduated with a double Master's Degree in French and Swiss Law and also holds a LL.M in European Legal Studies from the College of Europe.

Cecil Chung is Senior Foreign Counsel in the Seoul office of Yulchon LLC.

Linda Evans is a Partner in the Sydney office of Clayton Utz.

Juan Cristóbal Gumucio is a Partner in the Santiago office of Cariola Díez Pérez-Cotapos & Cía. Ltda.

Paul Lugard is a Partner in the Brussels office of Baker Botts L.L.P.

Evelyn Niitväli is a Partner in the Frankfurt office of RCAA.

Marc Reysen is a Partner in the Frankfurt and Brussels offices of RCAA.

Igal Schönberger is an Associate in the Santiago office of Cariola Díez Pérez-Cotapos & Cía. Ltda.

K K Sharma is Chairman of K K Sharma Law Offices in New Delhi, India.

Charles Weller at 69, is now in solo practice in Cleveland after Jones Day and Baker Hostetler .

German Zakharov is a Senior Associate in the Moscow office of ALRUD Law Firm.

David Cardwell is a Senior Associate in the Brussels office of Baker Botts L.L.P.

Karan Singh Chandhiok is a Partner in the New Delhi office of Chandhiok & Associates.

Jonathan Gowdy is a Partner in the Washington office of Morrison Foerster.

Christina Hummer is a Partner in the Brussels office of Saxinger Chalupsky & Partner Rechtsanwälte GmbH.

Mark Krotoski is an Assistant Chief in the Antitrust Division, U.S. Department of Justice .

Josselin Lucas is a Senior Associate in the Washington office of Paul Hastings LLP. He is a member of the Paris and Brussels Bars and licensed to practice as a Special Legal Consultant in the District of Columbia.

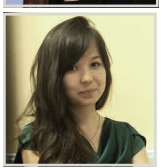
John Oxenham is a Co-Founder and Director of Nortons Inc. in Sandton.

Amadeu Ribeiro is a Partner in the Rio de Janeiro office of Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados.

Vanessa Jiménez Serrania is a PhD Candidate of the University of Salamanca and a member of the Madrid Bar. She is also a Senior Lecturer in European IP and Commercial Law at the Universities of Salamanca and Oberta de Catalunya.

Simina Suciu is an Associate in the Brussels office of Baker Botts L.L.P.

Koren W. Wong-Ervin is Counsel for International Antitrust in the Office of International Affairs at the U.S. Federal Trade Commission.



Alla Zhigaeva is a Junior Attorney in the Moscow office of ALRUD Law Firm.