Baker McKenzie.

Antitrust compliance

3 - 5 October 2023

ANNUAL COMPLIANCE CONFERENCE

Baker McKenzie.

Dawn raids and information gathering powers

Wednesday 4 October, 2.30 - 3.30 pm BST

ANNUAL COMPLIANCE CONFERENCE

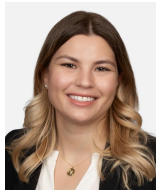
Speakers

James Robinson
Partner (Chair)
London
james.robinson
@bakermckenzie.com

Elisabeth Dehareng
Partner
Brussels
elisabeth.dehareng
@bakermckenzie.com

Lena Sersiron
Partner
Paris
lena.sersiron
@bakermckenzie.com

Sinan Diniz
Associate
Istanbul
sinan.diniz
@esin.av.tr



Ashley Eickhof
Associate
Washington D.C.
ashley.eickhof
@bakermckenzie.com

01 Scene-setting

Global antitrust enforcement trends

"Classic" cartel enforcement remains a priority

Rise of **"purchase"** cartel enforcement, including **no-poach** and other **HR** enforcement

Restrictions on **innovation, R&D, sustainability** efforts etc.

Increased enforcement of **EU/UK distribution rules** and **abuse of dominance**

Continued enforcement of cases involving **"information exchange"**, including use of AI/algorithms etc.

Focus on **personal liability** and **senior management** responsibility

02 Dawn raids – key updates

Dawn raids: the basics

Unannounced inspections at business premises and / or executive / employee homes

Suspicion of a competition law breach (e.g., cartel conduct, resale price maintenance)

Gathering of relevant information for subsequent investigation

Highly disruptive to the business

Can take place over several days and last long into the night

Data intensive (e.g., electronic data, personal devices/emails, hard copy documents)

The dawn of raids targeting remote working

Home raids are much more frequent

Increased risk of fines for obstruction / data destruction because of decentralisation of the raid

Senior IT employees and other key employees may need to travel to the offices as a matter of top priority

More data is copied with less effective shadowing, and rights of defence are "postponed"

Key principles remain the same: do not destroy, obstruct or mislead, but it's all about applying this to Data and Tech

Penalties and other risks

Effective management allows our clients to resume business more quickly

Individual criminal liability for obstruction

Mitigates damage to reputation

Obstruction attracts material fines (up to 1% of global turnover or uplift on substantive fine)

Issue-free raid helps build rapport with the regulator

Obstruction jeopardises leniency

Focus on Turkey: number of dawn raids and fines for obstruction on the rise

Year	Number of Dawn Raids
2020	502
2021	653
2022	831

Fines for obstruction of dawn raids on the rise

- From 2020 to 2022:
  - 65% increase in dawn raids
  - 2x more investigations
- Massive surge in fines for obstructing dawn raids since 2021
- Most of the dawn raid fines imposed occurred due to deletion of WhatsApp messages on cell phones
- The fines demonstrate that the increasing focus by the TCA on cell phone data and personal messages, as well as hybrid working arrangements where employees are called to the office for the dawn raid, create significant risks for companies

General investigatory powers

- Right to enter and search business and domestic premises, including offices, workspaces, desks and cabinets
- Inspectors have wide powers to obtain documents or information and may search and take copies of:
  - hard copy documents
  - electronic files (including retrieving deleted files and emails and running keyword searches)
  - storage devices (laptop/PC, phones, tablets, USB, servers, cloud services etc.) and text/WhatsApp/Signal messages
- Right to ask questions / interview employees / ask for written explanations
- Subject to legal privilege and scope of investigation
  - France – massive electronic seizures with a specific temporary closed seal procedure to exclude documents covered by legal privilege
- Duty to cooperate and not act in an obstructive manner during a dawn raid
- But some jurisdictional differences, e.g.,:
  - Turkey - potential requests for system-wide admin credentials
  - France – requests targeting employees that may be located outside of France – extraterritorial reach. Publication of a press release after dawn raid mentioning the targeted sector

Importance of data

Explain the
IT environment

Email accounts blocked and
copied (incl. deleted emails)

Laptops, phones (including
personal devices used for
work) handed over
for imaging

Server data
is imaged

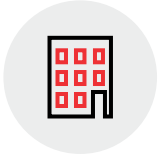
Admin credentials provided
to inspectors

Respond to
questions precisely
and accurately

Preparation steps to take now

Consider who would take on key roles in a dawn raid

- E.g., Internal Team Leader, IT Contact, Comms Team, Head of HR, key executives in Strategy Team
- Are these individuals normally on site? Consider possible replacements if someone is travelling
- Do you have their contact details easily to hand?
- Do you know where to get up to date personnel charts and organization charts?



What about other sites?

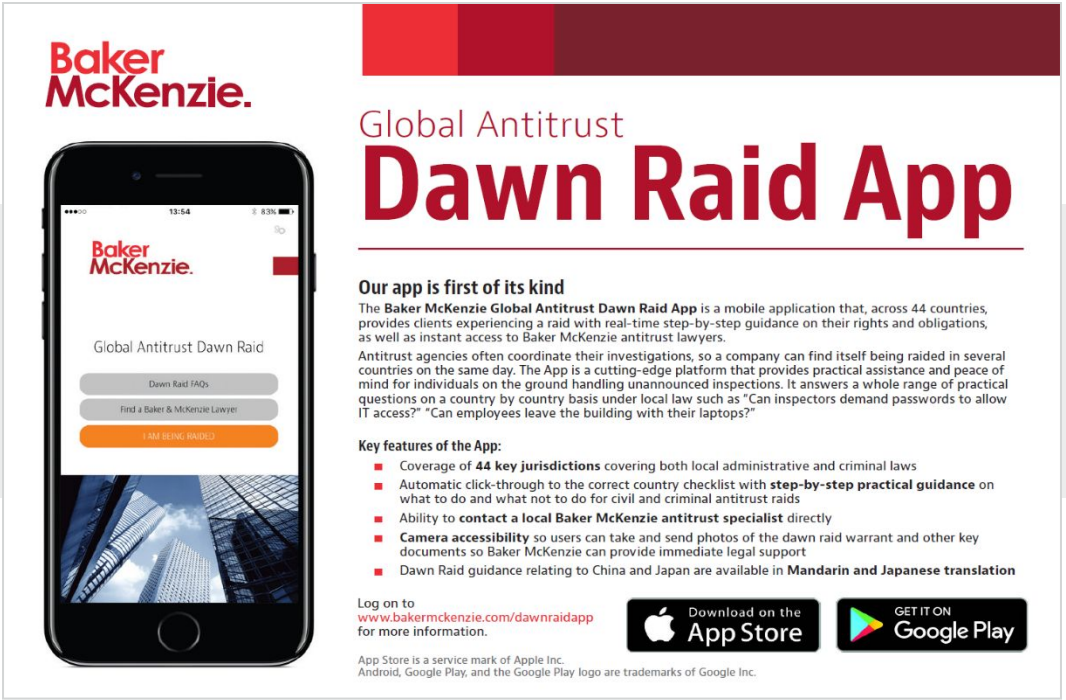
- Is Legal / IT / PA support available on site?
- If not, how quickly can personnel get there?
- What files / information is available at other sites?

Dawn raid guidance manual/mock raids

- Do you have a dawn raid policy/guidance in place and do employees know where to find it? Training?
- Would a mock raid be a helpful exercise to check whether employees have read/digested it?

Preparation steps to take now

Global Dawn Raid App



0 Subpoenas/information requests
3

Trends in US criminal enforcement

"First priority in corporate criminal matters is to hold accountable the individuals who commit and profit from corporate crime."

Prioritizing individual accountability, upward trend of enforcement of corporate executives

The Division has taken a number of steps to expand the scope of criminal antitrust enforcement (i.e., labor, AI)

DOJ have started to "flyspeck privilege logs much more carefully," scrutinizing parties who withhold information or delinquent in IR

Agencies sharpening their tools

"We're also working with the DOJ to address the increased use of third-party messaging platforms to send ephemeral or encrypted messages like disappearing chats - use of tools like that require additional diligence to preserve communications that are responsive to any demand."

Antitrust counsels should be "very vigilant" about ensuring that companies preserve internal employee online chats and other forms of informal communication.

Corporate Compliance and Enforcement

Criminal Enforcement Policies and Clawback Pilot Program

Clawback Pilot Program
Implement compliance related criteria to compensation structures

Compliance enhancements
(1) prohibition on bonuses for noncompliance; (2) disciplinary measures and (3) incentives for employees

Deferred Fine Reduction
Companies will receive fine reductions if they implement claw back compensation from culpable employees

- Individual Accountability
- Prior Corporate Misconduct
- Voluntary Disclosure
- Corporate Culture
- Independent compliance monitors
- Personal Devices and Third-Party Applications

"With a combination of carrots and sticks —with a mix of incentives and deterrence… empowering companies to do the right thing—and empowering our prosecutors to hold accountable those that don't."

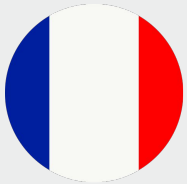
DAG Lisa Monaco, September 2022

Updates to DOJ Criminal Division policy on the collection of data from personal devices

Investigatory and cooperation challenges for companies

- Companies cooperating with DOJ should be prepared to answer questions about:
  - BYOD policies
  - Information about deletion and preservation policies.
- If company does not produce communications from third-party messaging applications - "ephemeral"
  - prosecutors can ask questions on access; location of information on company devices or servers; privacy
- Prosecutors will no longer take an inability to access this information "at face value" – could affect how company's cooperation is viewed

France: "simple" investigations coexist with dawn raids



- The French Competition Authority (FCA) may carry out "dawn raids", which require a Court order authorising widespread searches and seizures, or "simple investigations", which do not require a Court order
- Under the simple investigation procedure, FCA inspectors can visit premises without warning, carry-out interviews, consult documents and ask for specific documents which they know exist. They cannot search the premises
- This procedure is increasingly used by the FCA as easier to carry-out and no ability for the visited company to immediately lodge an appeal (appeal only allowed at the stage of the Statement of Objections)
- Simple investigations, though not authorised by a judge, are generally followed by significant requests for information and requests for documents – distorting this procedure

Turkey: far-reaching information requests

- In the recent Forex case, the TCA requested information relating to the parent company resident abroad by sending a RFI to the local subsidiary (i.e., chat logs of the 10 traders employed in the US and UK with largest trade volumes of TRY within the corporate group). This was justified by the argument that the parent company and the TR subsidiary constituted part of the same "undertaking"
- The TCA ultimately fined certain banks for not providing the relevant information
- The administrative court overturned the relevant fining decision for some of the banks based on the grounds that the service was not proper according to the Turkish Law of Notification (i.e., service should have been made to the parent company). This was later reversed by Regional Court of Appeals. Review by the Council of State (the highest administrative court) is ongoing.

UK: BMW v CMA

- Following Brexit, the CMA lost access to the European Competition Network's information channels
- In *BMW v CMA*, the CAT found that the CMA does not have the power to compel production of documents from foreign companies that do not have a sufficient UK nexus
- Potential significant impact on the CMA's ability to effectively conduct investigations under the Competition Act 1998
- CMA appealing judgment

We have no doubt that the CMA's construction renders section 26 of the 1998 Act aggressively extraterritorial. Because an "undertaking" is economic in conception, and because economic entities (particularly these days) will, more often than not, be international, and straddle and cross territories and borders, that is inevitable

BMW v CMA

04 Data privacy considerations

Why data privacy matters?

Emails, messages and other electronic communications data generated, sent or received by employees as part of their employment:

- qualify as personal data falling within the scope of GDPR, but also as electronic communications data subject to specific protection (ePrivacy/telecom)
- are protected, even if professional: in EU, employees have a right of privacy at work, including when using company IT resources (not possible to merely rely on "no expectation of privacy")
- employees are using company IT resources but also their own devices
- are usually key in investigations: either to respond to external requests/ orders from law enforcement authorities (external investigations), to collaborate voluntarily, but also internal investigations to establish, exercise or defend itself against legal claims
- risks of sanctions (admin fines under GDPR), but also civil and criminal actions, damage to reputation, prohibition to use evidence collected illegally in court

Main privacy/GDPR principles for any investigation

Lawfulness, fairness and transparency:
personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject

Purpose limitation:
personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible

Data minimisation:
personal data must be adequate, relevant and limited to what is necessary in relation to the purposes

Accuracy:
personal data must be accurate and, where necessary, kept up to date

Storage limitation:
personal data must not be kept in a form which permits identification for longer than is necessary for the purposes for which the personal data are processed

Integrity and confidentiality:
ensure appropriate security of personal data

Accountability:
the controller is responsible for and must be able to demonstrate compliance with GDPR

Key privacy aspects of external investigations

- Who is targeted by the request?
- Legal basis / lawfulness: legal obligation? legitimate interests? consent? necessary for the establishment, exercise or defence of legal claims?
- Transparency: do we need to inform the data subjects about a request from public authorities?
- Proportionality: scope of the search and data that can be disclosed
  - can we image laptops? phones?
  - what about personal devices? private/personal messages? personal email or instant messaging accounts?
- Use of third party provider? a data processing agreement will most likely be required
- Data transfer: restrictions to transfer data to a foreign country? foreign authority?
- Accountability: prepare a data protection assessment?

Key privacy aspects of internal investigations

- Identify the controller(s): who is deciding on the investigation ≠ who is the employer?
- Legal basis / lawfulness: legitimate interests? consent? necessary for the establishment, exercise or defence of legal claims? other requirements under ePrivacy/telecom secrecy?
- Transparency: ensure employees are duly informed (individually and collectively, if required)
- Proportionality: scope of the search and data that can be disclosed
  - can we image laptops? phones?
  - what about personal devices? private/personal messages? personal email or instant messaging accounts?
- Use of third party provider/e-discovery? licence? data processing agreement?
- Data transfer: restrictions to share data with parent/group company?
- Accountability: prepare a data protection assessment?

Preparation steps to take now

- Comply with GDPR, but also local data protection laws, employment and telecommunications laws
- Always use good judgement and follow the principles of transparency (inform employees individually and collectively) and proportionality (use the less intrusive means and apply a gradual approach)
- Have a comprehensive Employee Privacy Notice and clear IT & Monitoring Policy in place allowing access to employees' emails and other electronic documents (complying with local requirements, e.g., languages!)
- Implement a protocol/rules for data access (use key search terms to identify professional data that are relevant for the investigation and exclude non-relevant or private data)
- Ensure that any third party assisting with the investigation have appropriate license and put appropriate data protection agreement in place
- Do not forget that employees have a right to privacy at work. Not possible to say "No expectation of privacy!"

Questions

EU Foreign Subsidy Controls: practical implications for global businesses. Are you ready for 12 October 2023?

Thursday 5 October
2.30 - 3.30 pm BST
3.30 - 4.30 pm CEST
9.30 - 10.30 am EDT

Tomorrow's session