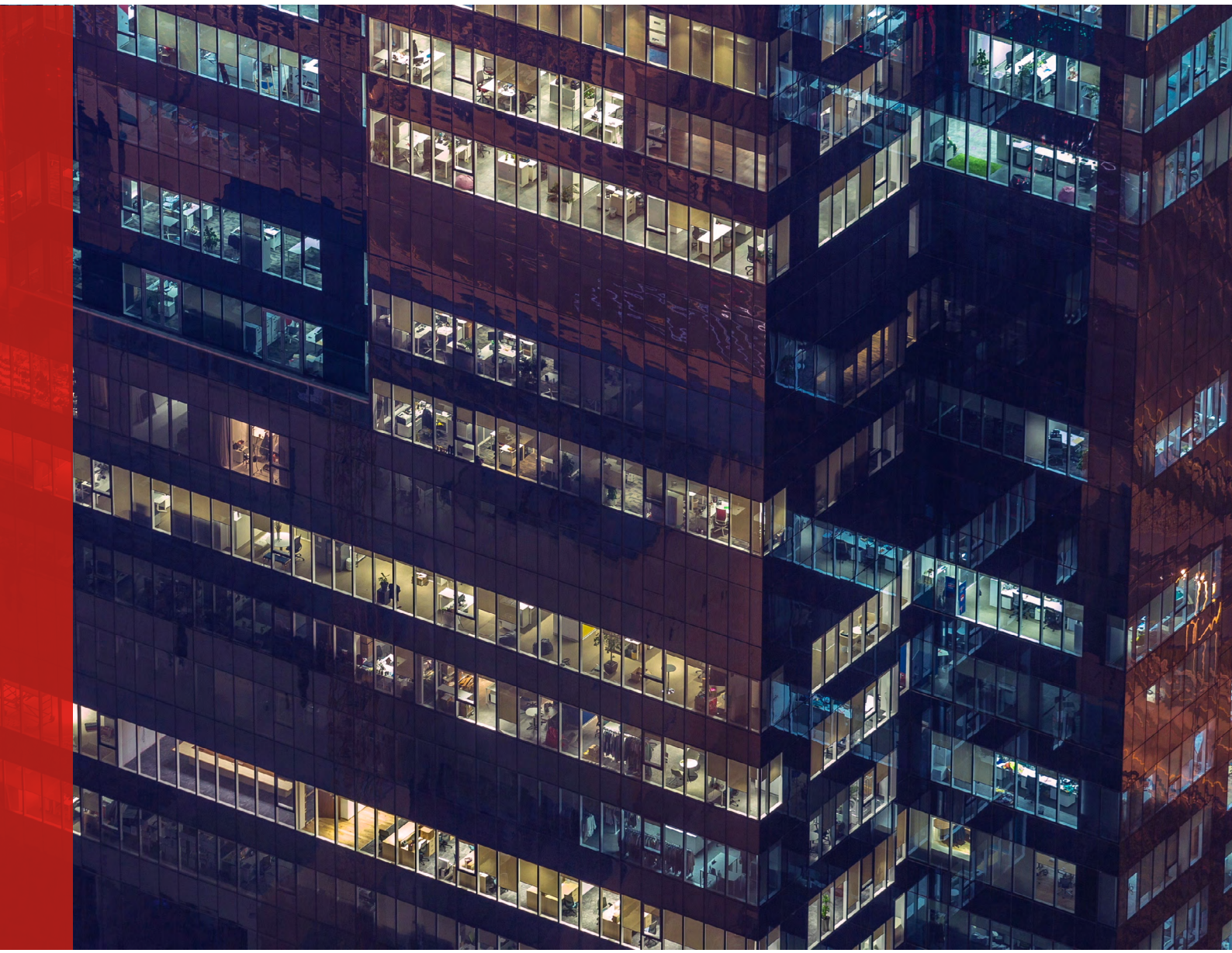
NORTON ROSE FULBRIGHT

Keeping your dawn raid guidance current



Why you should update your dawn raid protocols

Unannounced inspections or 'dawn raids' are used by antitrust authorities to obtain evidence when there are suspicions that individuals or businesses have infringed the antitrust rules. Often triggered by tip-offs from whistle-blowers or confessions from leniency applicants, dawn raids provide investigators with an opportunity to seize information for subsequent interrogation and review. The surprise element of dawn raids reduces the risk that evidence of a possible infringement will be destroyed.

Companies need to ensure their personnel are prepared for the possibility of a dawn raid, and that their protocols are adapted to an era where remote working is commonplace. Many businesses will have protocols including instructions for receptionists on what do to if investigators arrive and detailed guidance for compliance teams about the need to 'shadow' investigators as they move around the office and to photocopy all documents before they are taken away. The issue that protocols ought to cover in addition is how to prepare for and deal with forensic investigations, including when these are conducted remotely and/or at private homes.

How to prepare for, and respond to, digital forensic investigations, including at private homes

In a dawn raid, the investigators' key focus is to identify and seize electronically stored information (ESI). With businesses generating massive amounts of ESI each year, the authorities have developed sophisticated IT toolkits and procedures to manage the volume. Many enforcement agencies have dedicated forensic laboratories, skilled forensic investigators and the latest forensic imaging software, which they use to take images of servers, mobile devices and other IT media to capture ESI, including from cloud-based systems (e.g. OneDrive and SharePoint) and collaboration tools (e.g. Slack and Microsoft Teams).

Furthermore, some authorities are increasingly conducting remote dawn raids. This can involve the authority interacting with company personnel via video conference and downloading company data remotely after being granted access to the company's systems. In some cases, the officials may subsequently provide the company's external counsel with the opportunity to ensure documents are relevant to the authority's investigation by sharing their screens and allowing the external counsel to observe the officials filtering the documents so as to isolate those relevant to their investigation.

In the light of this new reality, companies need to update their dawn raid protocols to ensure their personnel are prepared for these changes.

Manage personnel's expectations

Company personnel should be trained on their obligation to cooperate with the authority's investigators to reduce the risk of the company being fined for 'obstruction.' In modern dawn raids, 'obstruction' is a broad concept. It is not limited to refusing to answer inspectors' questions during in-person interviews; destroying physical records; breaking seals placed by inspectors on individual offices and cabinets; blocking inspectors from accessing certain areas of the company's building; but can also include deleting electronic data; refusing to provide passwords; changing passwords; re-routing email traffic; blocking access to cloud-based storage areas; and refusing to be interviewed via video conference.

The IT director and team must understand what happens during a dawn raid

In a forensic dawn raid, the investigators will want to speak with the company's IT director (either in person or via video conference). To facilitate data collection, the investigators will need to understand the company's IT policies, IT systems environment and what ESI is held by key individuals or 'custodians'. Oftentimes, in-house legal and compliance teams will lack adequate knowledge of the details or the IT system administrative rights to enable the inspectors' ability to find and copy the ESI they seek. As such, the company's IT director and team need training, as they will be key players in the event of a dawn raid.

General considerations

If not already done, IT policies should be promptly updated and the company's personnel trained in relation to data retention, use of company IT systems and their obligations regarding company data. For example, if personnel save company related data to personal IT devices (e.g. home laptop, personal mobile phone/tablet, etc.), it would be more difficult for that employee to withhold such devices from inspection by officials should the employee be dawn raided at his/her private home. Where possible, employees should keep work devices separate from personal ones and avoid saving work material to personal devices.

Furthermore, the company's employees need training on how to respond if they are subject to a dawn raid at their private premises. For example, they need to know who to contact as well as their right to their own privacy and to ask the authority's investigators for a judicial warrant from a national court.

Is your business forensic dawn raid ready?

After getting the company's IT director and their team up to speed, the next step for the company is to familiarise its dawn raid response team with its IT systems.

This may be easier said than done, given that a company's digital filing cabinet may not be as neatly organised as it would like or expect. The company's servers could be in a different country from its offices. A third party could control access to the company's IT environment. Different system administrators could control access to different systems. The company may operate a host of legacy platforms that are understood by only a handful of people. All of these issues will take time to understand and map out. However, it is important to take action as soon as possible to avoid issues during a potential forensic dawn raid when the company may risk of being challenged with the accusation of obstructing the investigation.

Testing and trialling response scenarios is a good way to ensure the company's dawn raid response teams are well prepared. This can take the form of a Q&A session with representatives from the company's legal, compliance and IT teams to test how the company might respond to different scenarios. Additionally, the company may consider conducting a walk-through or mock forensic dawn raid to test its teams' response and resilience in providing ESI under controlled conditions, including strict time limits. The more prepared the company is to respond quickly and effectively when placed under pressure, the more robust its response will be in the event a dawn raid occurs. The emphasis in any dawn raid training has to be on resilience: the company's response team must be fully prepared for a (digital) forensic assault.

A practical example

Let's assume that the antitrust authority's investigators are looking for pricing strategy papers and associated correspondence relating to a new product launch. They have suspicions that the company has coordinated its strategy with one or more of its competitors. If asked where the business's commercial data for the last three years are held, its IT director will direct them to a range of possible company storage locations including email and document management servers (comprising cloud-based systems if applicable), laptops and mobile devices. The investigators then ask for a series of detailed technical questions to the company's IT director concerning how to access the servers; who the server administrators are; what the processes are for archiving documents and saving documents locally; whether the documents are encrypted; where to locate the mobile devices; and what the policies are about the use of personal devices for work purposes. This conversation lasts for just over an hour and is loaded with technical jargon and 'IT speak.'

Each member of the company's dawn raid response team must stay engaged in this discussion and be prepared to raise appropriate red flags. For example, a company's representative needs to explain credibly why there is no merit in capturing data over a three-year period given that the new product was conceived only 18 months ago. The company's lawyers will also need to make sure that the company does not, inadvertently, waive privilege over any legal advice received by the business concerning the legality of the pricing strategy. In the absence of these interventions, the company may find that the investigators seize far more data than is within scope. This lengthens the time the investigators are on site while they take forensic images – causing unnecessary disruption to business continuity. It also exposes the company's business to the risk that the investigators uncover other material that they use to pursue a new line of inquiry.

Each member of the company's dawn raid response team has a role to play, not only in cooperating with the authority's investigators, but also in understanding what is being asked of the company and responding appropriately to protect the company's position.

Top tips to get forensic dawn raid ready

1. Create an IT systems map showing where custodian data is held; how servers are organised; who controls access to data; the data format; and the limitations and restrictions on access to data. Determine whether the IT team can assist remotely or whether they would be needed on site in the event of a dawn raid.
2. Make sure that the company's dawn raid response team reviews and understands its information governance policies. Establish clear rules on the storage of data on local/end-user devices and on the use of personal devices for work purposes. Inform staff of what they should do if their home is dawn raided.
3. Provide guidance and training to IT staff on what information can and cannot be shared with officials. Equip IT staff to readily access passwords for encrypted hardware, software, folders or documents in the event of a raid.

Contacts

Claire Forster
Partner, Sydney
Tel +61 2 9330 8168
claire.forster@nortonrosefulbright.com

Alexandra Rogers
Partner, Head of Brussels
Tel +32 2 237 61 99
alexandra.rogers@nortonrosefulbright.com

Ian Giles
Head of Antitrust and Competition, EMEA, London
Tel +44 20 7444 3930
ian.giles@nortonrosefulbright.com

Eliot Turner
Partner, Houston
Tel +1 202 662 0200
eliot.turner@nortonrosefulbright.com

Marta Giner-Asins
Partner, Paris
Tel +33 1 56 59 52 72
marta.ginerasins@rtonrosefulbright.com

Tim Schaper
Head of Antitrust and Competition, Germany, Hamburg
Tel +49 40 970799 188
tim.schaper@nortonrosefulbright.com

Eric C. Lefebvre
Partner, Montréal
Tel +1 514 847 4891
eric.lefebvre@nortonrosefulbright.com

Marianne Wagener
Head of Antitrust and Competition, South Africa; Director, Cape Town
Tel +27 11 685 8653
marianne.wagener@nortonrosefulbright.com

Mai Muto
Counsel, Brussels
Tel +32 2 237 6140
mai.muto@rtonrosefulbright.com

Marc Waha
Head of Antitrust and Competition, Asia, Hong Kong
Tel +852 3405 2300
marc.waha@nortonrosefulbright.com

Our global offices

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

7000+
People worldwide

3000+
Legal staff worldwide

50+
Offices

Key industry strengths

- Financial institutions
- Energy, infrastructure and resources
- Transport
- Technology
- Life sciences and healthcare
- Consumer markets

Our office locations

Europe

- Amsterdam
- Athens
- Brussels
- Düsseldorf
- Frankfurt
- Hamburg
- Istanbul
- London
- Luxembourg
- Milan
- Munich
- Newcastle
- Paris
- Piraeus
- Warsaw

United States

- Austin
- Chicago
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- St Louis
- San Antonio
- San Francisco
- Washington DC

Canada

- Calgary
- Montréal
- Ottawa
- Québec
- Toronto
- Vancouver

Latin America

- Mexico City
- São Paulo

Asia Pacific

- Bangkok
- Beijing
- Brisbane
- Canberra
- Hong Kong
- Jakarta[1]
- Melbourne
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa

- Bujumbura[2]
- Cape Town
- Casablanca
- Durban
- Harare[2]
- Johannesburg
- Kampala[2]
- Nairobi[2]

Middle East

- Dubai
- Riyadh

1 TNB & Partners in association with Norton Rose Fulbright Australia

2 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com