HERBERT SMITH FREEHILLS

DIGITAL FORENSICS IN INVESTIGATIONS AND THE GROWING DATA BURDEN

21 July 2020 | Insight
– By **Stephanie Barrett, Arjuna Guruge, Elizabeth Macknay, Jeremy Birch and Jennifer Fong**

Businesses will need smarter data collection and management strategies to satisfy regulators

The approach to digital forensics in investigations is constantly evolving to keep pace with the increasing volume, velocity and variety of data within organisations. Almost every action we take leaves a digital trail and the type of information businesses are collecting, both internal and external, is expanding.

It is vital that businesses are alert to the challenges arising in an investigations context of how they acquire, hold and manage their data. With more data, comes the need for more careful planning, both before and after the commencement of an investigation.

"COLLECT EVERYTHING" IS NO LONGER AN OPTION

When scoping a collection exercise, the data locations and sources can be vast. As a result, there needs to be a focus around what is proportionate to collect and what should be prioritised. An instruction to "collect everything", while once-upon-a-time feasible, now could potentially mean terabytes of data and significant complexity around how to tap all potential sources.

Developing a smart data collection strategy that focuses on selective data sets is therefore imperative if businesses wish to avoid drowning in data. This strategy needs to be tailored to the purpose of the current investigation but with an eye to the future; taking into account the potential for an investigation to expand or for more expansive requests to be made by authorities. A distinction may be made between what to secure for future purposes vs what to collect now for processing and use in an investigation.

DATA AND INTERNAL INVESTIGATIONS – INSIGHT FROM OUR SURVEY
In our recent survey, over 60% of respondents said that the volume of data and the number of data sources used for internal investigations (or requests from regulators or law enforcement) has grown noticeably over the past two years, requiring more time and resources.
“The regulators are issuing very broadly drafted statutory notices which results in them obtaining a large amount of irrelevant material. They do not understand the size of the data held by large organisations nor the fact that the data is not necessarily held historically in a central location” (Survey respondent)

IT ALL STARTS WITH GOOD DATA GOVERNANCE

Managing the challenge of big data in digital forensics is made easier by having in place an effective data governance framework to begin with. A robust framework has a number of broad based benefits, including strengthening the usability and reliability of its data assets. A failure to maintain a sound approach to data governance creates problems when the business is facing the prospect of an investigation. First, it may expose businesses to risks, where keeping irrelevant, outdated or erroneous data may potentially hinder the analysis process of investigations and increase unnecessary costs. Second, businesses often run into problems with data integration, where the data needed for investigations comes from diverse sources, meaning that the need to remove duplicate documents and contradictory data may frequently arise.

At a high level three things are needed:

1. **Define the custodians of data assets** – a data steward oversees the life cycle of a particular set of data through establishing data quality metrics and ensuring the user community complies with the business' data governance policies.

2. **Establish key data metrics** that are designed to control data quality and to handle duplicates, inconsistencies and outliers.

3. **Establishing a master reference** which covers the data format, structure and range of adequate values, to ensure consistent use of data across all levels of the business.

RESPONDING TO GOVERNMENT REQUESTS

In the context of responding to government requests for data, whether by subpoena or dawn raid, it is important to consider cloud asset management. An organization should understand the location and access rights of its data held in the cloud.

With the proliferation of cloud storage in the corporate world, it is becoming more common for data relevant to a criminal investigation to be stored in a different jurisdiction. This has often resulted in a need to rely on mutual legal assistance treaties to obtain that data, which can slow down the investigative process. The US and the UK have both recently taken steps to address this situation, which may have a ripple effect, spreading internationally to prompt law reform and change practice in other jurisdictions.

In light of the increasingly prevalent use of cloud asset managements, the Securities and Futures Commission (**SFC**) has also set out the regulatory standard to be observed in Hong Kong, including amongst other requirements, that the external electronic data storage providers must be approved by the SFC. Some external electronic data storage providers may also have to provide an undertaking to provide the relevant records and assistance as may be requested by the SFC. It should be noted that irrespective of where the hardware for the storage information is located, all relevant records should be fully accessible upon demand by the SFC in a legible form without undue delay.

How to manage data stored in the cloud in the context of a dawn raid will depend upon the applicable laws of the jurisdiction where the inspection occurs. Government authorities and regulators are becoming more savvy when it comes to how the technology works and how best to obtain the information they need.

MANAGING DATA PROTECTION RISK

Data protection laws create challenges, particularly in cross-border investigations, due to restrictions on personal data that can be collected and transferred out of the jurisdiction. Despite the fact that approaches may vary across jurisdictions, the three most common modes where cross-border is permitted are:

Mindful of the various considerations, this risk can in most cases be sensibly managed.

SECRECY AND BLOCKING LAWS

Some jurisdictions have laws in place to restrict the disclosure of information altogether, particularly in the context of investigations. Such laws would prevent institutions from disclosing sensitive information after investigations have begun, with the hope of minimising resistance and potential jeopardy to the investigation. In the context of cross-border investigations, the operation of secrecy laws in one jurisdiction may cause issues with the compliance of disclosure obligations for regulators in other jurisdictions. Regulators in general, however, are becoming increasingly cooperative with each other; certain jurisdictions have specific legislation that provide for the sharing of information in investigations to facilitate the prosecution of crime.

By way of example, licensed corporations in Hong Kong have a statutory obligation under section 378 of the Securities and Futures Ordinance (SFO) to preserve secrecy relating to matters coming into their knowledge during the course of providing assistance to the SFC's supervisory functions. This obligation is strict and few exceptions apply, including disclosure required or authorized under the SFO, disclosure specifically exempted under the SFO, or communications with the SFC's consent. The SFC's consent is not required in a limited number of cases, such as for disclosure to an auditor for the purpose of preparing a report under the Securities and Futures Ordinance or to a solicitor for the purpose of seeking advice.

On the flip side, The People's Republic of China has recently enacted a law which could potentially prevent those based or working in the PRC from providing assistance in criminal proceedings outside the jurisdiction. Under that law, individuals and businesses are required to obtain approval from the Chinese government before disclosing evidence located in the PRC to overseas criminal enforcement authorities. Chinese authorities are also prohibited from seeking assistance from their overseas counterparts without obtaining a similar approval.

The evolution of data in the modern world has led to constant changes in both the practical aspects of data forensics in investigations as well as the change of law. Various countries in the world have amended their laws relating to privacy and investigations to adhere to the progression of data. In light of the diverse stages of development of relevant laws across different jurisdictions, it is important that businesses, especially multijurisdictional corporations, to ensure that they have a stringent data management process that accommodates data collection for investigations and other future uses.

EXPLORE OUR CAMPAIGN

SHARE

Share to Facebook Share to Twitter Share to LinkedIn Email Print
Show Share Links

RELATED TOPICS

Data and privacy

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

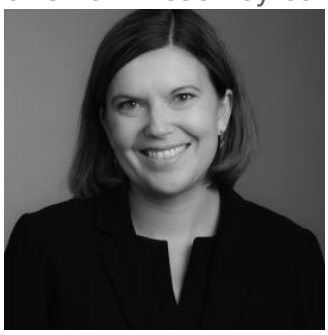
UPDATED: UK NATIONAL SECURITY ACT 2021 - WHAT INVESTORS NEED TO KNOW

Foreign investment: Rising tides of politics in regulation

Comply or Explain to climate-related reporting – A cross-industry roadmap

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



STEPHANIE BARRETT
HEAD OF EDISCOVERY & LEGAL TECHNOLOGY, UK, US & EMEA , LONDON
+44 20 7466 2536
stephanie.barrett@hsf.com

ARJUNA GURUGE
HEAD OF EDISCOVERY AND LEGAL TECHNOLOGY, AUSTRALIA & ASIA, MELBOURNE
+61 3 92881190
arjuna.guruge@hsf.com

ELIZABETH MACKNAY
MANAGING PARTNER, PERTH OFFICE, PERTH
+61 8 9211 7806
Elizabeth.Macknay@hsf.com

JEREMY BIRCH
PARTNER, HONG KONG
+852 21014195
Jeremy.Birch@hsf.com

JENNIFER FONG
SENIOR ASSOCIATE, HONG KONG
+852 21014244
Jennifer.Fong@hsf.com