REPRINT

corporate disputes

TECHNOLOGY FORENSICS IN FRAUD INVESTIGATIONS AND DISPUTES

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
APR-JUN 2018 ISSUE

corporate disputes
APR-JUN 2018
www.corporatedisputesmagazine.com
Inside this issue:
FEATURE
UK and UPC ratification
EXPERT FORUM
Challenges when enforcing arbitral awards
HOT TOPIC
Litigation in the pharmaceutical and medical device sector

BROWNRUDNICK
an international law firm

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

MINI-ROUNDTABLE

TECHNOLOGY FORENSICS IN FRAUD INVESTIGATIONS AND DISPUTES

PANEL EXPERTS

Jane Colston
Partner
Brown Rudnick LLP
T: +44 (0)20 7851 6059
E: jcolston@brownrudnick.com

Jane Colston is one of the award winning 14 litigation partner team at Brown Rudnick London combining cross border civil fraud, criminal and regulatory experience under one roof. The team won in 2018 the Legal 500 award for civil fraud litigation. Ms Colston has acted in numerous complex, cross-border fraud cases and has extensive experience of forensic investigations. She has managed numerous cases involving freezing, search, disclosure, gagging and delivery up injunctions.

Aaron Pickett
Digital Forensic Examiner
IT Group UK
T: +44 (0)845 226 0331, ext 505
E: aaron.pickett@itgroup-uk.com

Aaron Pickett is a digital forensic examiner who specialises in computer and mobile investigations in both the civil and criminal sectors as well as cyber security. He has worked on cases involving employee theft, ransomware attacks, fraudulent activities as well as cases involving burglary, employee misconduct and money laundering.

Tom Epps
Partner
Brown Rudnick LLP
T: +44 (0)20 7851 6010
E: tepps@brownrudnick.com

Tom Epps is also one of the partners in Brown Rudnick's award winning litigation team. He is recognised in the UK and internationally as a leading white-collar crime lawyer specialising in business crime and regulatory investigations. He has been a partner with Brown Rudnick since July 2013 and has been involved in many of the UK's largest and most complex fraud investigations and prosecutions over the last 20 years.

Kieran Maher
Assistant Digital Forensic Examiner
IT Group UK
T: +44 (0)845 226 0331
E: kieran.maher@itgroup-uk.com

Kieran Maher is an assistant digital forensic examiner who specialises in computer and mobile investigations, alongside crucial expertise in web technologies. He has worked on cases involving post-breach remediation for online retailers, employee theft and the fraudulent doctoring of medical documentation.

CD: Could you provide an overview of how information recovered from digital technologies may contribute to evidence in a fraud investigation or dispute?

Colston: If you act for a claimant, seeking to obtain relevant data from dishonest defendants early on is essential to successfully tracing stolen assets and identifying the co-conspirators or those who, innocently or otherwise, hold relevant data. Search, freezing and Norwich Pharmacal disclosure orders (NPOs) are civil court 'weapons' of first choice to achieve this. These civil orders are designed to obtain data by catching the targets unaware so they do not have time to hide or destroy the data. Internet service providers (ISPs) and banks are also frequent targets for NPOs in order to obtain, without notice to the account holder, full details to help trace stolen monies and establish the wrongdoers or the wrongdoing. It is true there is significant frontloading of legal costs but such orders give you a lot of 'bang for your buck' and often accelerate an early disposal of the case.

Epps: If you are acting for a company under investigation by a UK enforcement agency, such as the Serious Fraud Office, you could feed electronic copies of documents into advanced fraud analytics engines which use artificial intelligence (AI) to get to the key information fast. That targeted insight is then available to the company under investigation so it can prioritise documents that should be looked at first and therefore get ahead in understanding what has happened. The 2017 High Court decision on the scope of legal professional privilege (LPP) in the ENRC case (*Director of the Serious Fraud Office v Eurasian Natural Resources Corporation Ltd*) has, in practice, made defence lawyers in white-collar crime investigations think particularly carefully about creating new data, such as interview notes, since those notes or statements made by an employee during an internal investigation may not be privileged.

Maher: Data recovered from devices are often the backbone of fraud investigations. This is because typical data on a device can reveal much more information than an individual might at first imagine. For example, an image on a mobile phone does not contain just the date it was taken, but often the location coordinates pinpointing where the image was taken. Documents likewise contain similar metadata, often storing much more information than a user would first consider. Combining this metadata that is generated from almost every action on a device, with chat analysis from popular messaging applications, can more often than not be the foundation on which a fraud investigation is built. Deleted data likewise proves an invaluable resource, as actually deleting a file from a device is much more complex than one would initially believe.

Pickett: Recovered data could prove vital as part of a fraud investigation. Information from desktop and laptop machines can reveal documents, and associated metadata, for further analysis that can reveal forgery of documents, communication or images. Adding this to the plethora of data available from mobile phones – both the location through cell site analysis and information downloaded from the device – can often reveal motives and methods used to conduct fraud. Timeline forensics can particularly be important when cross-referencing against key times and dates, such as the receipt of an email from a 'fake' email account at the same time that one is sent from suspects' computers.

CD: What fraud investigation techniques and procedures are typically deployed to gather evidence from technology to prove wrongdoing, particularly in cases where data has seemingly been erased, corrupted or destroyed?

Maher: There are a few key tools employed in forensic investigation, where an individual is believed to have deleted files or deliberately corrupted them. There is the process of data carving. Almost all investigations into fraud begin with a data carving process. This process allows us to recover deleted data and files, potentially going back to the birth of the device. While metadata is usually lost as a result, the content of the file usually remains integral and can therefore serve as part of the investigation. There are also processes and resources available that will attempt to mend or fix deliberately corrupted and broken files, such as when an individual tries to delete an email account from a device.

> "Data recovered from devices are often the backbone of fraud investigations. This is because typical data on a device can reveal much more information than an individual might at first imagine."
>
> *Kieran Maher, IT Group UK*

Pickett: One of the first stages of an examination where there is a suspicion that data has been erased would be to check for 'anti-forensic' tools. In the assumption that these have not been used, a carving exercise is conducted. This technique often gathers long-deleted files, but will not be able to recover dates and file names. Despite this, the method will often recover evidence of wrongdoing and malicious deletion of files. Similarly, the investigation of documents and associated metadata often reveals key artefacts that can lead to a successful conclusion of a fraud investigation. During the creation of any documents, a whole host of file system and embedded metadata is created. It is a well-known fact among many forensic professionals that one of the key members of the hacking group 'Anonymous' was caught using this method. Despite being well-known for hiding behind many layers of digital anonymity, a simple check of a press release document showed that the author, Alex Tapanaris, had left his real name in the metadata.

Colston: Hunting down the places where relevant data is hidden is a challenge. Often you are lucky, such as a chance remark or the wrongdoers being observed at the right time. Often you make your own luck, for example by getting search orders. This, however, requires a significant legal budget and a coordinated team of fraud litigators and forensic investigators that will image the seized e-data. Even when search orders have been obtained, thoroughly searching all the hiding places is a substantial exercise requiring tenacity. It also requires a thorough knowledge of where data can be hidden. Technology helps locate devices, as often they 'talk' to each other or a WiFi will identify other devices logged onto it.

> **"Technology helps locate devices, as often they 'talk' to each other or a WiFi will identify other devices logged onto it."**
>
> *Jane Colston,*
> *Brown Rudnick LLP*

Epps: Forensic investigators may be able to check whether the target's computer or laptop has had deletion software installed on it. If so, it is still possible to identify the type of files deleted. The analysis forensic investigators perform will also reveal USB and other devices connected to the target's computers and laptops to see if data was potentially copied to them. As fraudsters may well prefer to hide rather than destroy data, those forensics can usefully open a line of enquiry to uncovering the data. In one case, a Google map was found during the search on a suspect's PC which ultimately led to the recovery of a laptop which had been thrown into a lake. A forensic investigator was nonetheless able to recover about 60 percent of the data on the laptop.

CD: What legal and regulatory considerations need to be made when assessing the hardware or data of a suspected criminal? Are there any challenges or barriers which may complicate the process?

Colston: A civil search order will prescribe the scope of the search that can be done and the data that can be seized and reviewed. The supervising solicitor on a search order is there to seek to ensure compliance with the order, for example so that legal privilege is safeguarded. Stepping over the line of what is court sanctioned would likely be a contempt punishable by imprisonment. To ensure admissibility of data recovered, the Association of Chief Police Officers' (ACPO) 'Good Practice Guide for Digital Evidence' should be and is usually followed. From a criminal perspective, the search warrant will typically define what is permissible. Those advising defendants should consider whether on any *ex parte* application for a warrant the police complied with their duty to provide full and frank disclosure to the court. Failure to do so would expose the police to a court challenge, as would overstepping the scope of the search warrant.

Epps: UK enforcement agents must also take particular care regarding documents that are journalistic materials, subject to commercial confidentiality or subject to legal professional privilege (LPP). Generally, LPP material must not be reviewed. The defence team must therefore engage at a very early stage with the enforcement agency to ensure LPP material remains unsighted. The suspect is nearly always well-advised to hold a very firm position in that regard throughout the initial exchanges. This is particularly important where the police exercise their powers – under Part 2 of the Criminal Justice and Police Act 2001 – during a search to seize large volumes of material and sift them later for the documents within scope of the warrant. Robust screening procedures must be put in place to prevent any infringement of a client's LPP, and they should seek to reach an agreement with the relevant agency, at the outset of the raid itself, about handling of LPP material.

Pickett: One of the key barriers to assessing data associated with any suspected criminal is the Human Rights Act. Any digital device that is analysed will have personal data on it, which could include communications with loved ones, family photographs or social media web history. Any of these artefacts could be seen as impacting upon an individual's human rights, hidden among a mountain of digital data that could prove or disprove a particular theory. Another area that is often not considered is the Computer Misuse Act. If there is no court order, there is no authority to take any laptop and examine it for evidential artefacts. Adequate permission must be received from the court or the device's owner, which could be the user or the business owner, prior to the analysis of the laptop, or else the examiners themselves would be in breach of the Computer Misuse Act.

Maher: The legality of an investigation is constantly at the forefront of an investigator's mind. Before any investigation can be conducted, the Computer Misuse Act is considered, to be certain the person handing over the evidence is the owner of the data. During investigations all parties must remain vigilant to ensure evidence is kept secure and out of publicly accessible arenas. This is because, if an investigator were to allow the evidence to fall into the public domain, they might be found to be breaching the Data Protection Act, and not respecting the privacy of the individual being investigated.

CD: Given the sensitive and volatile nature of digital data, do you foresee established standards and processes for collecting, storing and preserving data struggling to keep pace?

Pickett: The standards and processes involved in the collecting, storing and preserving of data

are, for the most part, adequate measures that are proving to be relatively timeless. After all, no matter how the data is stored, it is ultimately a collection of ones and zeros, as it always has been. The ACPO guidelines provide a well-established methodology for collecting, storing and preserving the data that continues to be relevant. Despite this, more and more information is being stored in the cloud, causing problems where the collection of this evidence is important. New standards would be useful for collecting this data, which often proves troublesome, especially in cases where employee theft through cloud services such as OneDrive or DropBox is concerned. This is likely to become even harder with the upcoming General Data Protection Regulation (GDPR) further limiting the amount of information that can be stored, and where, and who can access it.

Colston: The principles in the ACPO's Guide have so far stood the test of time. For example, that no action should be taken which changes data which may be subsequently relied upon in court, and those accessing original data should be competent to do so and be able to give evidence explaining their actions and by reference to a clear audit trail. Given that this is fast changing, the guide will need to be periodically evaluated to ensure it remains fit for purpose. It is also key that those who specialise in fraud litigation keep pace with what technology can do and where data can be hidden and work knowingly with legal engineers to exploit the AI systems available.

Epps: Technology has to be used to cost-efficiently mine data, otherwise the volume of data is likely to be overwhelming and the case, whether civil or criminal, prohibitively expensive to fight and slow to resolve. Those who fail to skill up may lose out to opponents who are using it and they may fail to gain significant insight into the modus operandi of some law enforcement agencies that are using it. We fully appreciate the significance, for example, of the Serious Fraud Office (SFO) having deployed AI – specifically, the RAVN software – to examine extensive batches of data to help identify particular material in the course of their corruption investigation regarding Rolls-Royce PLC. The SFO was reported to have said that the technology was “more effective, more efficient and more accurate than human intervention”. I understand, the SFO agreed to the use of RAVN to help identify and then quarantine documents subject to LPP. Using such technologies means cases could well be investigated quicker than if they were investigated manually. They are an enabling tool for the sifting, and then analysis, of huge volumes of data.

Maher: A lot of the industry is already subjected to well-established standards. A prime example would be ISO, with many organisations ISO 27001 and ISO 9001 accredited. This means they are audited every year. In addition, there are the ACPO guidelines. These guidelines apply throughout any investigation, from the acquisition of data, through to the storage of such data. Furthermore, the new GDPR comes into force in May of this year and we have already begun preparations to be certain we comply in every way. While this poses a particular challenge for us internally, with reference to who can access which files, it is a welcome new safeguard, as the GDPR will further ensure we are taking every step we can to not only keep up to date with best practice in our field, but also keep our case data as safe and secure as possible.

CD: Once data has been recovered, what processes need to be undertaken to evaluate and maintain its integrity?

Pickett: Hashing processes are used to ensure that the integrity of data is maintained throughout the analysis of the recovered data. Created by running algorithms across data, be it a full hard drive or a single file, a hash is the digital equivalent of a fingerprint, with a change in a single byte of data dramatically altering the hash value. A hash is taken at the time of imaging, and this hash value is regularly checked and regenerated to ensure continued integrity. As a second layer of protection, any work conducted on evidence is conducted in a read-only format. This means that the data recovered will never be altered as the write-blocking devices will not allow any changes to the files being worked upon.

Maher: The process of acquiring data using modern techniques will almost always allow for the generation of hashes. With a hash taken at the time of imaging, we can then reference back to this at any point in an investigation, to ensure the integrity of the data and make sure nothing has been changed in the evidence. A large portion of, although not all, forensic images are stored in a particular file format called an E01. This universally recognised format adds an element of safety in that we can be certain various tools and software are handling the evidence correctly, due to the established standard of the E01 format. Evidence handling standards likewise ensure the integrity of data, and allow any individual to be able to track the past movements of a piece of evidence.

Epps: Suspects, whether that be in the context of civil or criminal litigation, will usually challenge provenance of the data and examine in some detail the way in which the data has been handled throughout the investigative process. Many enforcement agencies are legally obliged to record and retain material which may be relevant to their investigation. As such, a clear audit trail must be kept as to what was done to evaluate the data. Such evaluation may then be done using Technology Assisted Review (TAR) – machine learning (ML) algorithms which evaluate and help to determine the relevance of documents. However, it is worth bearing in mind that the quality of ML is naturally informed by the quality of the human guidance and input, and we foresee vigorous challenges may well be pursued by criminal defence teams in relation to the integrity and cogency of the process. While we see a greater role for digital forensics in fraud investigations, there remains an absolute premium placed on making sure the right technology is managed very carefully and used in the right way.

> **“Many enforcement agencies are legally obliged to record and retain material which may be relevant to their investigation.”**
>
> *Tom Epps,*
> *Brown Rudnick LLP*

Colston: In respect to evaluating the data, the English civil courts in the 2016 case of *Pyrrho Investment v MWB Property* have already sanctioned the use of TAR. This is different from keyword searching and manual review by humans. Based on the human training TAR receives, it searches for patterns, common and related concepts, meaning of words, idioms and context to find other relevant documents in the data set. It is intelligent in the sense that it makes decisions based on the data's analysis as to whether a document is relevant to the issues in the case or covered by privilege. TAR can be used on language-based data, including foreign languages.

CD: To what extent do anti-forensics techniques such as encryption frustrate fraud investigators? Is the involvement of a digital forensics expert always a must-have component of a fraud investigation?

Maher: Encryption will always be an issue when it comes to forensic investigation. Strong encryption is becoming commonplace in the industry, and for the most part is good practice to keep data safe. However, it is not fool proof. Specialised tools exist to break encryption algorithms, and while not always effective and rarely quick to run, they do allow us to at least attempt to break through the barrier of modern encryption. There are many anti-forensic techniques besides encryption. Fortunately, most of these techniques prove fruitless in the modern era, as tools and programmes exist that allow us to detect such attempts to hide or delete data.

> **"Encryption is one of the leading frustrations for digital forensic investigators. Despite this, encryption cracking techniques have improved that can combat this issue."**
>
> *Aaron Pickett,*
> *IT Group UK*

Pickett: Encryption is one of the leading frustrations for digital forensic investigators. Despite this, encryption cracking techniques have improved that can combat this issue. This does rely on some idea of the users' password length or type to achieve results on a low budget and there is no guarantee of success. Many 'traditional' anti-forensic techniques – such as hiding data in bad clusters or changing the Master Boot Record to hide partitions – typically no longer cause problems for forensic investigators. Newer techniques and tools will look over all bytes on the machine, not just 'good' sectors and partitions specified by the Master Boot Record for files, evidential artefacts and hidden partitions.

Colston: A digital forensics expert is essential on the execution of search orders or warrants. In respect of WhatsApp data, for example, although this is now fully encrypted from point-to-point, as long as you seize the phone and obtain the iTunes username and password for the iPhones, the data can be captured by the digital forensics expert in a decrypted format during the forensic process. A search order will usually require the target to disclose user names and passwords and give access to all devices and email accounts. Failure to do so would be a contempt of court. The civil courts have recently been prepared to imprison those who have defied its orders and have been willing to do so for up to two years. Freezing, disclosure and search orders can be used to compel a defendant to disclose his assets, including whether he has received stolen monies in the form of bitcoins.The question is whether a defendant will comply with such order and what you can do if he does not.

Epps: If disclosure is not made, the challenge is finding out about assets not mentioned, such as bitcoins owned by the defendant. NPOs are unlikely to assist, as the whole point of virtual currencies is that there is no intermediary from whom to seek disclosure. However, the defendant can be compelled by a court order to disclose bank account statements in order to see if bitcoin-related purchases have been made from online merchants or an exchange. Furthermore, the imaging and analysis of data obtained from a search order may show if the defendant's private bitcoin key and wallet are stored on his computer and, if so, you may be able to view the user's blockchain transactions with his co-conspirators.

CD: Looking ahead, do you expect digital forensics to play an even greater role in fraud investigations? What trends are on the horizon?

Epps: TAR is still regarded with some scepticism but increasingly we will see it used. Document review has, of course, evolved over the years. It was not long ago that white-collar crime investigations began and often ended with sifting papers in archive boxes. Nowadays, all reviews are primarily electronic. The use of AI software is therefore simply a logical and necessary next step. The key challenge is how to harness AI most effectively. We are the generation that will and must master that skill. While one size will not fit all, and not every case will benefit from using AI, to ignore the advantages that AI brings or to fail to understand how enforcement agencies are using AI, is an increasingly outdated approach.

Pickett: Fraud involving digital devices is increasing. In some aspects, techniques that fraudsters can use have multiplied exponentially thanks to the advances in document creation, new communication techniques and the ability to hide activities through layers of anonymity. I expect this trend to continue to grow as fraudsters exploit new technology. One of the biggest trends on the horizon is the growth of blockchain technology. The decentralised, but potentially huge, computing power could assist investigators by allowing them to compare evidential artefacts or find potentially-falsified communications by comparing them with proven-legitimate communication stored on a blockchain ledger. An example of this potential development can be seen with the introduction of KODAKCoin for assisting photographers protect their image copyrights using blockchain technology.

Colston: Keeping up to speed with new technology is crucial to ensure your civil order is fit for purpose. The English civil court has been willing to adapt its orders to be responsive to changing circumstances. For example, given it is possible to download what has been heard in the target's household on an 'Alexa' device, the civil courts may be willing to authorise access by a claimant. In regard to any imaging order, it is key that the case's forensic expert reviews any draft order to check it works from a practical point of view. For example, some cloud service providers throttle how quickly data can be downloaded so the order must deny the defendant access during this time.

Maher: We do believe that due to the ever growing and expanding market, forensics will continue to grow within fraud investigations. Throughout the field of commercial technology, more and more devices are emerging at an increasing rate, and yet there remains no uniformity across these devices. That is to say, to investigate two phones by two different companies would require two different skillsets. The rate at which forensic tools can keep up with innovation is increasing, but it still requires manual input and knowledge of the respective field to know which technique of investigation would be appropriate and where. The trends seem to point towards an increased usage of encryption and similar methods of obfuscation. Relating this back to fraud, encryption algorithms can be used to prevent fraud at the source, as we see today in banking and large organisations. CD