The long arm of HMRC

Adam Craggs and Alice Kemp outline the powers HMRC has at its disposal when conducting a criminal rather than civil investigation

Most readers will be familiar with the powers available to Her Majesty's Revenue & Customs (HMRC) to compel the provision of documents and information from taxpayers and third parties, such as banks and accountants, in the context of a civil HMRC enquiry[1]. What might be less well-known is HMRC's ability to obtain communications data when investigating suspected criminal activity.

Tackling serious organised crime is a priority for HMRC and access to communications data has a vital role to play in meeting that challenge. Under Part 3 of the Investigatory Powers Act 2016 (the IPA), HMRC can request data held by telecommunication operators including the time, duration and location of a telephone call, together with the number dialled ('communications data'). It cannot, however, without the authority of the Secretary of State, ascertain what is being said on the call. This is sometimes described as the 'who', the 'when' and the 'where', but not the 'what'.

Following a Freedom of Information request from our firm RPC, HMRC has confirmed that in 2019 it made 18,464 requests to access communications data; up slightly from the 2018 total of 18,263 requests and a significant increase from the 11,513 requests made in 2010.

With the increase in home working as a consequence of the Covid-19 pandemic, communication data takes on an even more significant role and we anticipate that the number of requests from HMRC for communications data will increase further in 2020 and 2021.

In the context of suspected furlough fraud, HMRC might wish to access communications data to ascertain whether any business calls have been made or received by business mobile telephones issued to furloughed employees. Similarly, HMRC might be interested to learn whether furloughed employees' mobile telephones were located at business premises when the employees made or received a call.

But what about the contents of emails and text messages?

Because of the broad wording of the IPA, 'communications data' does include emails and instant or 'text' messages[2]. But whereas telephone calls and websites tend to be 'in the moment', and leave no lasting record[3], emails are different. Most people tend to keep a record of the emails they receive on their telephone, tablet, laptop or personal computer, which means that there is another aspect to consider – HMRC's ability to access stored data.

There are a number of ways in which HMRC can, in the context of a criminal investigation, access emails or messages stored on electronic devices, but the main ones to be aware of include:

the special procedure material provisions contained in Schedule 1 and section 14 of the Police and Criminal Evidence Act 1984 (PACE), which can be used to compel the disclosure of material in the possession of a person or organisation, created or acquired in the course of business, held subject to an obligation of confidence or secrecy and likely to be of substantial value to the investigation of the commission of an indictable offence;

search warrants issued pursuant to section 8 of PACE, to search and seize material (which will normally include computer servers, electronic devices and mobile telephones) located at a specified address (such search warrants are typically issued in relation to both business premises and private residential addresses).

Do you have to provide your password or encryption key?

Of course, in order to comply with various data protection requirements and as a protective cyber security measure, many electronic devices are password-protected and encrypted, which can cause difficulties for investigatory bodies

---

1 See Schedule 36 to the Finance Act 2008.

2 There are additional provisions which relate to internet connection records (see section 62 of the IPA).

3 Unless there is an interception warrant issued under Part 2 of the IPA. This is a complex area of the law and outside the scope of this article.

such as HMRC. If a person refuses to provide a password, or encryption key, to enable investigators to access lawfully obtained information, they can be compelled to do so. HMRC can issue a notice to that person pursuant to section 49 of the Regulation of Investigatory Powers Act 2000 (RIPA). **Section 49** provides the power to serve a **notice** on a person who is believed to be in possession of a password or encryption key, to provide that password or key within a specified period of time. A knowing failure to comply with a section 49 notice is a criminal offence punishable by an unlimited fine and/or a term of imprisonment of up to two years.[4]

COP 9 as an alternative to a criminal prosecution

While the investigative powers described above are designed to provide evidence that might underly a criminal charge, HMRC is in a different position to most other regulators and prosecutors in that its focus is primarily on the collection of tax revenue.

As a consequence of this differing focus, even when HMRC suspects tax fraud and is in possession of evidence which might justify a criminal prosecution, it may nonetheless choose to go down the Code of Practice 9 (COP 9) route rather than commence a criminal investigation. COP 9 is a civil procedure used in selected cases where HMRC suspect tax fraud but do not wish to carry out a criminal investigation with a view to prosecution. The taxpayer is given the opportunity to make a full disclosure under a contractual arrangement called a Contractual Disclosure Facility.

The factors influencing the decision by HMRC as to whether to proceed by way of COP 9 or criminal investigation where fraud is suspected are many and varied and the presence of communication data may be a factor in the decision-making process. For example, where HMRC is in possession of information from the seizure of emails or relating to the use business mobile telephones, which suggests fraud, it may nonetheless form the view that it will better serve the public interest to offer a COP 9 investigation rather than initiating a criminal investigation.

However, in our experience, cases where a COP 9 is offered after communications data is obtained are very much the exception. Obtaining communications data or a search warrant are all significant steps that can only be undertaken by HMRC if there is no reasonable alternative method of acquiring the information sought. This means that, in practice, a decision to conduct a criminal investigation with a view to a subsequent prosecution is likely to have already been made.

It is important to obtain appropriate specialist legal advice should you become aware that any of the above investigative steps have been utilised by HMRC.

Adam Craggs is a partner at RPC LLP. He can be contacted on 07545 101 656 or at adam.craggs@rpc.co.uk

Alice Kemp is an employed barrister at RPC LLP. She can be contacted on 07852 633 754 or at alice.kemp@rpc.co.uk

[4] Or up to five years in cases involving national security or child indecency (see section 53(5A)(a) of RIPA).