Department for the Economy
www.economy-ni.gov.uk

176 Newtownbreda Road
Belfast
BT8 6QS
Telephone: 028 9025 3955
Text Relay: 18001 028 9052 9900
Fax: 028 9025 3953
Web: [redacted]

Mr Lee Jefferson
[redacted]

Date: 10 January 2016

DfE Ref No. 2016-0154

Freedom of Information (Freedom of Information Act 2002) Request

Thank you for your request for information relating to the Investigatory Powers Act 2016. The request was received on 9 December 2016 and the Department is dealing with it under the terms of the above legislation.

You have asked for information held on file (if any) which explains why the Department needs access to the data gathered in the Investigatory Powers Act 2016. The Department does not hold this information on file, however I can confirm that this information is already in the public domain as provided in the attached link to the Home Office Publication, **Operational case for the use of communications data by public authorities,** (such as the Department for the Economy in Northern Ireland).

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536331/operational-case-for-the-use-of-communications-data-by-public-authorities.pdf

You may wish to note the opening sentences of Paragraph 2, page 9 "Communications data can often provide a crucial, and sometimes the only, evidential lead. For example, communications data from a mobile phone operator can allow a trading standards department to identify a rogue trader targeting the vulnerable, and subsequently assist in a successful prosecution". The Department for the Economy is responsible for the trading standards service in Northern Ireland which enforces legislation aimed at tackling rogue traders in Northern Ireland.

I have enclosed an Access to Information Factsheet which provides information on FOI procedures, including what to do if you are not happy with our response, and some useful contact points.

Yours sincerely

DENNIS CUNNINGHAM
Consumer Affairs Branch

Department for the Economy
www.economy-ni.gov.uk

Access to Information Fact Sheet

Note: This leaflet gives an overview of some of the main provisions of the Freedom of Information Act and Environmental Information Regulations and should not be regarded as a legal interpretation.

1. What is the Freedom of Information Act? The Freedom of Information (FOI) Act 2000 was fully implemented on 1st January 2005, giving you the right to request information from public authorities. This allows you to access information about how the Department works, spends public money, reaches decisions, etc.

Information may also be obtained under:

- **The Data Protection Act 1998 (DPA)** - this allows you access to information held *about you* by both public and private organisations, and gives you the right to make sure it is correct.

- **The Environmental Information Regulations 2004 (EIRs)** - This legislation gives you access to any environmental information held by organisations that perform public functions.

2. How do I get information about Department for the Economy under these Acts? You can find information on the Department's website: https://www.economy-ni.gov.uk. If you can't see what you're looking for you can contact us by email at [redacted] or write to us at:

Information Management Unit
Department for the Economy
Netherleigh, Massey Avenue
Belfast BT4 2JP

Please state your name, address, telephone number and specific details of the information you require.

3. How long does it take to get information under the FOI Act? Once a written request for information is received, we will respond promptly, and at any rate, within 20 working days. In certain circumstances a final response may be made outside this period where additional time is needed to determine whether or not disclosure would be in the public interest.

4. Is there a cost? This depends on a number of factors including the volume and complexity of material requested. Responses to enquiries that cost the department less than £600 to process[i] will be provided free of charge, although there may be a small charge for disbursements[ii]. The Department has a right to refuse an FOI request if the cost of locating and retrieving the information exceeds £600. We will not refuse a request for environmental information on the grounds of cost alone; however we have the right to charge a reasonable amount to cover processing costs. In all cases, we will notify you of any estimated costs before proceeding with the request.

5. What happens if the information I want is not available? The Department is not obliged to create or acquire information it does not already hold, but we will try to assist where possible. We may contact you about what relevant information we do hold, or may offer to transfer your request to another public authority that might help.

6. Can I have any information at all? The FOI Act and Environmental Information Regulations allow you access to much of the information held by public bodies. But some types of information are exempted, for example personal details about others, or where disclosure might prejudice a company's commercial interests.

7. What if I am refused information? We will tell you if information is being withheld and why. If you are unhappy with how we have handled your request you have the right to request an internal review. To request an internal review send an email or letter within 40 working days, to our Head of Information Management Unit – see contact details at point 2 above.

We will reply to you within 20 working days. If you are not satisfied with the result of the internal review you may appeal to the Information Commissioner (details provided below at point 9). The Commissioner will normally expect an internal review to have been carried out prior to appeal.

8. How do I find out more? More information is available from office of the Information Commissioner at:

Website:	www.informationcommissioner.gov.uk	**Phone:**	[redacted]
Post:	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF	**Email:**	[redacted]

Re-use of Information

Some information supplied to you under the FOI Act may continue to be protected by copyright. You are free to use it for your own purposes, including private study and non-commercial research, and for any other purpose authorised by an exception in current copyright law. Documents (except photographs) can be also used in the UK for the purposes of news reporting without requiring permission. Any other re-use, for example commercial publication, would require the permission of the copyright holder.

Most documents produced by government departments will be protected by Crown Copyright and most Crown Copyright information can be re-used under the Open Government Licence. Further details are available on the The National Archives website. Copyright in other documents may rest with a third party. For information about obtaining permission from a third party, see the Intellectual Property Office's website at www.ipo.gov.uk.

[i] Includes the cost of locating, retrieving and extracting the information
[ii] Disbursements may include costs of photocopying, printing, postage etc

Operational case for the use of communications data by public authorities

Contents

Public authorities' use of communications data

The purpose of this document is to explain why public authorities need the ability to acquire communications data and to show that only those authorities that can make a compelling case are provided access to communications data under the Investigatory Powers Bill.

This document is split into two sections. The first section provides key facts explaining what communications data is and the safeguards that govern access to that data. It then outlines the general requirement for public authorities to access communications data, explaining how they have a crucial role in fighting crime and protecting the public that cannot simply be passed to the police. The first section concludes by explaining how internet connection records can assist these authorities in their investigations into online criminality, in particular in identifying the real world sender of online communications through the resolution of internet protocol (IP) addresses.

The second section of this document provides an explanation for why each of these specific authorities needs to be able to acquire communications data. It provides specific case studies demonstrating how the data has been used successfully in investigations, including to help convict serious criminals, locate vulnerable people and identify the cause of fatal accidents.

The public authorities covered in this document are the authorities David Anderson, in his report, *A Question of Trust,* referred to as the 'minor users of communications data'. He supported their ongoing ability to acquire communications data and this document builds on the justification for their powers.

While these authorities do, on average, acquire communications less than the police and security and intelligence agencies, access to communications data is still fundamental to their work. For example, the case studies in this document show how the Serious Fraud Office has acquired communications data to identify individuals involved in the top tier of bribery and corruption. They show how the National Offender Management Service used communications data to identify a corrupt prison officer and how the Air Accident Investigation Branch discovered, through the acquisition of communications data, that a helicopter pilot was using his phone at the time of a fatal crash. The crimes the authorities this document covers investigate are not trivial, they include offences such as defrauding vulnerable people of their life savings, stealing sensitive personal information and supplying dangerous counterfeit medicines. In short, this document explains why it is absolutely essential they are able to acquire communications data.

References

Where clauses are referred to in this document they relate to the Investigatory Powers Bill as brought to the House of Lords (HL Bill 40, 2016-17). This document refers to the operators that provide telecommunications and postal services as ‘communications service providers’. The definitions of postal and telecommunications operators are provided by clauses 233 and 234 of the Bill.

Key facts

- Communications data – the who, where, when and how of a communication but not its content – is a vital tool used to investigate crime and protect the public. It is used in 95 per cent of serious and organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division and has been used in every major Security Service counter-terrorism investigation over the last decade.

- Under current legislation, the Regulation of Investigatory Powers Act 2000 (RIPA), communications data has been essential to a wide range of public authorities. For example, it helps the Financial Conduct Authority to investigate insider trading and the Maritime and Coastguard Agency locate people lost at sea.

- Communications data can only be acquired where it is necessary in a specific investigation for a particular statutory purpose (which must have been approved by Parliament), and it may only be acquired where it is proportionate to what is sought to be achieved.

- The Investigatory Powers Bill, currently before Parliament, will update the legislative framework for the acquisition of communications data and strengthen the safeguards. Schedule 4 to the Bill sets out the public authorities that can acquire communications data. This is the first time that all the authorities that will be able to acquire communications data have been included on the face of primary legislation, providing for full Parliamentary scrutiny of the list of public bodies able to acquire communications data.

- In his 2015 report, *A Question of Trust,* David Anderson QC recommended that "public authorities with relevant criminal enforcement powers should in principle be able to acquire communications data. It should not be assumed that the public interest is served by reducing the number of bodies with such powers, unless there are bodies which have no use for them."[1]

- The Government regularly reviews which authorities should have access to communications data and removes authorities that are not able to make a sufficiently strong case for access. 13 such authorities were removed in February 2015.

- In relation to the Investigatory Powers Bill, the Home Office required all relevant authorities to make the case that they needed powers. The Home Office carefully considered those cases and made further changes to the bodies that have access to communications data. This included removing access from the Prudential Regulation Authority and restricting the purposes for which some authorities could acquire data.

[1] "A Question of Trust: Report of the Investigatory Powers Review" David Anderson QC, p. 295, Para 50

Safeguards for the acquisition of communications data

There are robust safeguards that apply to any application for the acquisition of communications data, which are being further strengthened by the Investigatory Powers Bill.

- Communications data can only be acquired where it is necessary in a specific investigation for a particular statutory purpose, and it is proportionate to what is sought to be achieved.

- A public authority can only acquire data for a statutory purpose that relates to their specific responsibilities.

- All applications must be made through a single point of contact (SPoC). The SPoC's role is to ensure effective co-operation between relevant public authorities and communications service providers, and to facilitate lawful acquisition of communications data.

- Once the application has gone through the SPoC, it must be approved by a designated senior officer (DSO) of a rank approved by Parliament and who must be independent of the investigation.

- Oversight of use of the powers will be provided by the Investigatory Powers Commissioner, who must hold or have held high judicial office.

- The Investigatory Powers Commissioner must keep the use of investigatory powers by public authorities under review and report annually on the use of the powers. Where the Commissioner becomes aware of a relevant error, the error must be reported to the person to which it relates.

- Furthermore, any individual who thinks that surveillance powers have been used against them unlawfully can apply to the Investigatory Powers Tribunal to review their case.

- A detailed statutory code of practice sets out the practices that must be followed by public authorities who acquire communications data.

- The Bill contains a new offence of knowingly or recklessly obtaining communications data from a communications service provider without lawful authority. The offence attracts a maximum penalty of 2 years' imprisonment and will provide a firm check against abuse of communications data powers.

The authorities covered in this paper

In his report, *A Question of Trust,* David Anderson QC reported that the police and security and intelligence agencies make 99 per cent of communications data applications. The other one per cent are made by what he referred to as the 'minor users'.[2] These users include authorities as diverse as local authorities, the Criminal Cases Review Commission and the Financial Conduct Authority (FCA). In 2014 these authorities made around 1,000 applications for communications data which resulted in roughly 7,000 requests to communications service providers.[3]

These figures are not spread evenly amongst all authorities. Some of these authorities will very rarely need to acquire communications data. For example, the ambulance and fire services need the power in limited circumstances where they may need to locate someone in an emergency. However, other authorities, such as the FCA who investigate, among other things, insider dealing, acquire communications data more often than many small police forces. Essentially, while these authorities make relatively few requests, their requirement to be able to acquire communications data is absolutely fundamental.

This paper explains why each of the authorities needs to be able to acquire communications data. It does not cover authorities where the requirement for investigatory powers is already well known. The authorities who are able to acquire communications but are not included in this document are the police, security and intelligence agencies, Her Majesty's Revenue and Customs, the Home Office (for border and immigration investigations) and the Ministry of Defence.

While the vast majority of the bodies already have access to communications data, the Investigatory Powers Bill is the first time that primary legislation has ever set out the bodies with the ability to acquire communications data. This is an important step in improving transparency and providing explicit Parliamentary approval for the acquisition of communications data by public bodies. The relevant provision of the Investigatory Powers Bill is Schedule 4 which sets out:

1. the public authorities that will be able to acquire communications data;

2. the minimum rank of designated senior officers within those authorities who are permitted to authorise the acquisition of communications data;

3. the types of communications data that may be authorised by each designated senior officer;

4. the statutory purposes for which communications data may be obtained e.g. 'for the purpose of preventing or detecting crime or of preventing disorder'.

---

[2] Ibid, p.166, Paras 9.2 – 9.3

[3] "Report of the Interception of Communications Commissioner March 2015 (covering the period January to December 2014)", HC113: 'Annex B: Total Applications, Notices & Authorisations for each Public Authority under Chapter II of Part I RIPA 2000'

In total, Schedule 4 to the Bill contains 47 entries, making up between 550 and 600 public authorities (of which over 400 are local authorities).

Safeguards specific to minor users of communications data

There are potential benefits in some authorities requesting communications data through the SPoCs and designated senior officers in other authorities that acquire communications data more frequently. This is because, inevitably, those authorities that request data most frequently will be able to build up more experience and expertise in acquiring communications data, thus reducing the possibility of errors or inappropriate use.

The Bill therefore provides for 'collaboration agreements' that will allow infrequent users of communications data to make their applications through more frequent users. The Bill also creates a power for the Secretary of State to direct relevant public authorities to enter into such collaboration agreements.

Safeguards specific to local authorities

There are a number of additional safeguards that apply specifically to local authorities.

- All local authority communications data requests must be approved by a magistrate;

- Local authorities can only acquire communications data for the purpose of the prevention or detection of crime;

- All local authority requests must be made by SPoCs in an independent body – the National Anti-Fraud Network. This means that individual local authorities are never allowed to approach communications service providers directly to request communications data. The Investigatory Powers Bill enforces this by requiring local authorities to be part of collaboration agreements;

- Specific provision in the Investigatory Powers Bill to prevent local authorities from acquiring internet connection records.

Why communications data powers are required by a range of public authorities

Although they make a relatively small number of requests for communications data, it is nonetheless important that the public authorities detailed in this document are able to acquire the data, where it is necessary and proportionate to do so. These bodies have a mandate from Parliament to investigate certain offences and ensure public safety. Importantly, the Bill only permits them to acquire communications data for statutory purposes that relate to their specific responsibilities. For example, most public authorities can only acquire communications data for the purpose of 'preventing or detecting crime or of preventing disorder', whereas the Financial Conduct Authority will be the only authority permitted to acquire communications data for the purpose of 'exercising functions relating to the regulation of financial services and markets, or financial stability'.

Communications data can often provide a crucial, and sometimes the only, evidential lead. For example, communications data from a mobile phone operator can allow a trading standards department to identify a rogue trader targeting the vulnerable, and subsequently assist in a successful prosecution. Requests will often be very limited and would simply involve asking the operator which of their particular customers owns a certain phone number. Alternatively, it might involve the Air Accident Investigation Branch determining if a pilot was using their phone when a plane crashed. However, even such limited requests must meet stringent tests of necessity and proportionality.

Why it is not appropriate for the police to acquire communications data on behalf of these authorities

As this paper explains, Parliament has given these authorities responsibilities to investigate certain offences. It is not appropriate to decide that where investigation of those offences requires communications data they should be handed over to the police. In many cases, the police neither have the resources nor the specific knowledge, such as the relevant training, to take on such investigations. However, as explained below, the collaboration agreement provisions would allow the Secretary of State to require public authorities to make their applications through a different authority, if that is deemed appropriate.

Joint investigations

There may be circumstances, for example when a crime reaches a certain level of seriousness, where it is appropriate for these public authorities to work with the police, or hand over cases to the police. However, this does not mean that these authorities have no need to acquire communications data in their own right, since often it will be impossible to identify the seriousness of a case without the initial evidence communications data provides. This can be demonstrated through the following case study.

In May 2016, restaurant owner Mohammed Zaman was found guilty of manslaughter and six food safety offences. This followed a customer having an allergic reaction to peanuts in a product that he had ordered and had specifically requested no nuts.

The conviction followed a joint investigation by the police and the trading standards department of North Yorkshire County Council. The investigation involved the use of communications data. The defendant denied that he knew various matters during interview. However, phone records were used to show that he had been in touch with staff and suppliers at various points.

As this case involved manslaughter, the police acquired the communications data. However, had the case only involved the food safety offences, it would not have been a joint investigation and the council would have acquired communications data on their own - the food safety offences in themselves amounted to an 18 month sentence. For issues, such as food safety, it is important they can be investigated before they escalate to more serious offences when the police need to be involved. While this case is an example of circumstances where an investigation took place after a tragic incident, it clearly demonstrates that it is appropriate that authorities, such as local authorities and the Food Standards Agency, should have powers to investigate these offences in the early stages.

Online criminality

This section explains why the authorities in this document will need to carry out online investigations and, in particular, be able to use internet connection records.

More and more offences, such as the sale of illegal goods, are taking place online. Equally, criminals (like everyone else) increasingly communicate through online services such as apps on their mobile phones, rather than through traditional telephony. These authorities, just like the police and intelligence agencies, therefore need the tools to tackle such online criminality. For example, in relation to the Gambling Commission, David Anderson said in his report: “betting fraud is often conducted online and can only be tackled through an investigation online”.[4]

Tackling online criminality often requires the resolution of IP addresses. IP address resolution is the ability to identify who in the real world was using an IP address on the internet at a given point in time and therefore who was the sender of an online communication. An IP address is automatically allocated by a network provider to a customer’s internet connection so that communications can be routed backwards and forwards to the customer. This might involve, for example, determining the identity of a rogue trader offering services online.

Why internet connection records are needed for IP address resolution

The Government has been consistently clear, including in the ‘Operational Case for the Retention of Internet Connection Records’ published alongside the Bill[5], that internet connection records are needed to resolve IP addresses in certain circumstances.

[4] “A Question of Trust: Report of the Investigatory Powers Review”, p. 184, Para 9.80
[5] Available at: https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents

When a public authority needs to identify the user of an IP address, they will always know the specific internet service that was used in advance of the application. They will just need to identify the individual who carried out the activity on the internet service. This is made absolutely clear in the Bill (clause 59(4)(a)). IP address resolution does not therefore involve determining the website a person was using, it involves determining the individual who carried out an action on an already known website. For example, IP address resolution can involve identifying the specific individual selling illegal goods online – this could be the IP address used to put an advertisement on a website. The internet service the individual was using to sell the goods would already be known so the application for communications data would be to determine which individual was using that internet service at the time the illegal goods were put on sale. In short, the question the public authority would ask the communications service provider would be:

> 'who was using this IP address on this specific internet service at 1300 on 5 Jan 2016.'

The communications service provider would need to process information showing that the particular internet service had been used (including the internet connection record) but it would only need to disclose which individual was allocated the specific IP address.

It would not therefore make sense to restrict the use of internet connection records by these public authorities. It would not prevent the authorities making applications to resolve IP addresses. The question they would ask the communications service provider would be as follows:

> 'who was using this IP address at 1300 on 5 Jan 2016.'

Not including the specific internet service in the request would make it harder for the IP address to be resolved and make it more likely that there would be collateral intrusion in what was disclosed by the communications service provider. This is because, where IP addresses are shared between numerous users, not including the internet service in the request would make it much more difficult for the communications service provider to identify solely the specific user the public authority is interested in because they would not be able to immediately exclude all other users of the IP address that were using different internet services.

Furthermore, if such authorities were restricted from using these powers, the only route available for continued investigation would be for the case to be handed over to the police. It would not be appropriate for offences that take place online to be handed to the police for the same reasons it would not be appropriate for the police to acquire communications data on behalf of other authorities more generally. Equally, it would not be appropriate for these authorities to be able to acquire communications data when the offence involves a phone call but to be required to hand it over to the police, or for it not to be investigated, where there is an online element.

Public authorities

When deciding which authorities should be able to acquire communications data under the Investigatory Powers Bill, the Home Office required all the authorities in this document to provide evidence of their need for the power, including through case studies.

The below sections include a sample of the information that these authorities provided. As explained above, it does not cover the police, security and intelligence agencies, Her Majesty's Revenue and Customs, the Home Office (for border and immigration investigations) or the Ministry of Defence.

In terms of devolved authorities, the Home Office's starting position has been that, where powers are needed, devolved authorities should have the equivalent powers of their English counterparts, unless there are specific reasons to deviate from this. Where the case studies below cover more than one authority that is because the case studies should be taken to demonstrate the need for both the English authority, as well as the relevant devolved authority.

At the beginning of each section there is a table setting out the specific entries in Schedule 4 to which the case studies relate, the statutory purposes for which those authorities can acquire communications data, the total number of applications for communications data and the number of notices and authorisations those applications amounted to in 2014.[6] The figures provided below are taken from Annex B to the "Report of the Interception of Communications Commissioner, March 2015 (covering the period January to December 2014)".

[6] The Acquisition and Disclosure of Communications Data Code of Practice 2015 explains the difference between authorisations and notices in more detail. In short, an authorisation granted to a member of a public authority permits that person to engage in conduct relating to the acquisition of communications data. A notice given to a postal or telecommunications operator requires it to disclose the relevant communications data held by it to the public authority.

Ambulance services

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Ambulance trusts in England • Northern Ireland Ambulance Service Health and Social Care Trust • Scottish Ambulance Service Board • Welsh Ambulance Services National Health Service Trust
Statutory purposes under clause 58(7) available to these authorities
• (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health
Communications data applications covering the period from January to December 2014
• Applications: 0 • Notices & authorisations: 0

Requirement to be able to acquire communications data

The ambulance services may need to acquire communications data in an emergency to prevent death or injury.

Sometimes people get disconnected when contacting the emergency services. This could be for a number of reasons such as low battery, poor signal or a phone being damaged or taken as part of an incident. There will also be circumstances where a person in difficulty may be unable to describe their location with sufficient accuracy for the emergency services to locate them. Communications data can be used to assist the emergency services getting to a person in time.

In practice, the ambulance service very rarely acquire communications data under the Regulation of Investigatory Powers Act 2000 (RIPA) and that is likely to continue to be the case under the Investigatory Powers Bill. This is because the Communications Act 2003 requires certain communications service providers to provide communications data to the emergency services following an emergency call made to 999 and 112 emergency numbers. There is a period of one hour after the termination of an emergency call in which access to the data for the emergency services falls outside the provisions in RIPA and in the Bill. The ambulance services have been provided powers in this Bill in case they need to acquire communications data in an emergency outside of these circumstances.

Competition and Markets Authority

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Competition and Markets Authority
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• Applications: 2 • Notices & authorisations: 2

Requirement to be able to acquire communications data

Under the current legal framework the Competition and Markets Authority (CMA) acquires communications data in the course of investigating suspected breaches of the criminal cartel offence in the Enterprise Act 2002. Cartels are the most serious form of anti-competitive conduct.

The cartel offence is a serious crime with a maximum sentence of five years imprisonment and an unlimited fine upon conviction on indictment. It may be thought of as a type of fraud for financial gain, in which individuals collude to fix prices, carve up markets, or rig bids in order to cheat customers of the benefit of competition. Cartels typically have the effect of artificially raising prices for customers, which can be by as much as 30 per cent or more. The victims of such conduct may be businesses, consumers or, in the case of public contracts, taxpayers, who either end up paying more or being unable to afford the affected goods or services.

Cartels are typically carried out in secret, with often elaborate steps taken to conceal them. As awareness of the CMA's enforcement activity increases and as communications technology becomes more sophisticated, we can expect those involved in criminal cartel activity to turn to new and more sophisticated methods of communicating so as better to conceal their conduct and reduce the likelihood of detection. To date, the CMA has been able to use its existing communications data powers to link individuals together, both to corroborate other evidence or intelligence and to support applications to use other forms of evidence gathering powers, including more intrusive powers such as surveillance using covertly placed listening devices. This can be particularly valuable in cartel cases, which will often involve secret meetings between competitors.

Because of the complexity and resource-intensive nature of cartel investigations, the CMA carries out a relatively small number of operations. However, communications

data plays a key role in the detection and investigation of illegal cartels and effective enforcement on the back of such investigations is critical to deterring such cartels and to enabling the CMA to fulfil its mission to ensure markets work well for consumers, businesses, and the economy. Such activity in turn supports economic growth and wider confidence in the market.

Case study 1:

Communications data required: Telephone subscriber and billing data

Background / Reason for requesting data: A leniency application (the CMA has a policy of granting lenient treatment to businesses or individuals who inform it of cartel activities) was received by the CMA, in which the applicant provided information about a criminal cartel. The applicant provided details of the co-conspirators and also stated when the next cartel meeting was to be held.

Communications data (both subscriber and billing) was obtained not only to prove connections between the individuals, but also to corroborate the initial information provided by the leniency applicant. Once the meeting venue was known a directed surveillance authority was granted and a listening device planted in the room. At the same time a number of search warrants were applied for and issued by the High Court for business premises, based in part upon the connectivity established from the telephone data obtained.

Outcome: Following the successful recording of the cartel meeting, all of those concerned were arrested and search warrants executed, which led to additional documentary evidence being obtained at the premises. All concerned were charged with the cartel offence and appeared at Southwark Crown Court where the communications data formed a key part of the prosecution case. The trial resulted in one of the defendants being convicted.

Would the outcome have been achieved without the data: The communications data was crucial in corroborating the initial information provided by the leniency applicant. Without this it is quite possible that the High Court would not have issued the search warrants, not being content to rely upon uncorroborated 'single strand' intelligence. Therefore, without the communications data, it is quite possible that the other evidence would not have been found and the prosecution would not have taken place.

Set out below are two 'composite' example case studies based upon the CMA's experience to date. They are intended to illustrate the different initial stages of intelligence-led investigations into criminal cartel activity, using a range of investigative tools, including communications data.

Case study 2:

Communications data required: Mobile phone subscriber and billing data.

Background / Reason for requesting data:

The CMA's cartels hotline receives information that a cartel is operating in the medical supplies industry. The source states that Mr Jones (Company A) is fixing prices with Mr Smith (Company B) and another unknown company in the supply of medical equipment to the NHS. The source has overheard Mr Jones talking to Mr Smith on his mobile telephone and thinks they have agreed to fix prices within a current tender process and that this practice has been going on for years.

The source supplies the telephone number used by Mr Jones and agrees to act as a covert human intelligence source (CHIS). Results of a subscriber check on the number confirms that Mr Jones is the subscriber to the telephone and a further request is made for Mr Jones' billing data. Analysis of the billing data shows a number of calls during working hours to two distinct numbers. Further subscriber checks on these numbers show one number belonging to Mr Smith and the other belonging to an as yet unknown individual (Mr Black).

Other enquiries confirm Mr Black is an employee of Company C. Further billing data shows that all of the identified numbers are in regular contact and that they are all calling a fourth number at regular intervals. Subscriber checks on this number confirm the telephone owner as a Mr Williams.

Other enquiries confirm that Mr Williams is an NHS employee. The authorised CHIS thinks that a meeting is being planned in the near future to discuss and finalise contracts. Other powers are used to obtain credit card records and confirm that a local hotel has been used in the past. Discreet enquires are made and a private room booking is discovered in the name of Williams. A covert listening device is placed into the private room. Mr Jones is followed to the hotel and seen to enter the room with the other suspected cartelists. The conversation is recorded and provides evidence confirming the cartel / bid rigging activity.

Outcome: All those concerned are arrested and searches under warrant are carried out on the business premises to discover additional evidence.

Would the outcome have been achieved without the data:

Unlikely. The CMA would not have been able to establish a link between those concerned in the first instance without a significant risk of prejudice to the investigation – requiring Mr Jones to produce his own telephone records would likely have led him to tip off the other conspirators unknown to the CMA at the time (Mr Black or the corrupt public official Mr Williams). Without the data identifying Mr Williams, it is likely no credit card data could have been sought in a timescale to allow the meeting venue to be identified in advance, if indeed the meeting had gone ahead given the likely tip off if Mr Jones had been sent an information notice, leading to the loss of the direct evidence (covert recording) needed to prove the case.

Case study 3:

Communications data required: Device identifier, subscriber and billing data

Background / Reason for requesting data: A source has informed the CMA that individuals are fixing bids for contracts and as such are adding 20 per cent to the cost of high value public road building programmes. The source states that the individuals involved in the suspected criminal cartel are using ‘pay as you go’ mobile telephones to contact each other. The source names the main cartelist as Mr Smith.

Enquiries identify Mr Smith’s telephone and a subscriber check reveals that the telephone is a ‘pay as you go’ telephone. An application for traffic data reveals that the user is only calling four other numbers. Subscriber checks on these reveal four further ‘pay as you go’ numbers with no subscriber details. A further traffic data application confirms that all of the numbers are only calling each other and are not connecting to other known telephone billing.

The source states that those concerned have regular meetings to agree prices but that he cannot ascertain when the next meeting will be. Additional enquiries reveal where the cartel meeting is taking place and a listening device is placed in the meeting room of a local hotel.

Outcome: The meeting is recorded and provides direct evidence of the cartel offence. Following arrest, all of the mobile telephones are recovered and the billing data previously obtained proves that the cartelists have been in regular contact with each other.

Would the outcome have been achieved without the data: Unlikely. Without the communications data, the CMA would likely have been unable to establish the telephone numbers being used by the cartelists and link the conspirators together. First, Mr Smith would likely have tipped off his co-conspirators if he had been required to produce his telephone records. Second, the other conspirators may not have responded truthfully to information requests sent to them since the relevant phones were pay as you go (rather than registered handsets / lines).

Criminal Cases Review Commission

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Criminal Cases Review Commission • Scottish Criminal Cases Review Commission
Statutory purposes under clause 58(7) available to these authorities
• (h) to assist investigations into alleged miscarriages of justice
Communications data applications covering the period from January to December 2014
Criminal Cases Review Commission: • Applications: 2 • Notices & authorisations: 2 Scottish Criminal Cases Review Commission: • Applications: 0 • Notices & authorisations: 0

Requirement to be able to acquire communications data

The Criminal Cases Review Commission (CCRC) is the independent body responsible for the investigation of potential miscarriages of justice in England, Wales and Northern Ireland. It has the power to refer cases back to the appropriate appeal court if it decides that new evidence or argument gives rise to a “real possibility” that the court would not uphold the conviction or sentence. It can also be directed to carry out specific investigations by the Court of Appeal.

The CCRC acquires communications data in order to assist with its investigations into alleged miscarriages of justice. It helps the CCRC to review cases where people may have been wrongfully convicted and may ultimately lead to miscarriages of justice being corrected by the courts. For example, communications data demonstrating contact between individuals can amount to new evidence which undermines the safety of a conviction. Alternatively, communications data that identifies an individual can help the CCRC to identify new witnesses or other potential lines of inquiry that might not have been available at the time of the trial. With the increase in communication over the internet, the CCRC needs to be able to access internet connection records if such an issue arises in a case.

Communications data can also assist the CCRC in reaching a decision not to refer a case for another appeal; for example by undermining the submissions made by an applicant or discrediting a potential new witness. This is equally as valuable to the

CCRC and the Criminal Justice System as a whole because a flawed decision to refer a case would cause unnecessary distress to the victim(s) of the crime in question.

Due to the nature of the CCRC's work it is not always possible or desirable to approach a subscriber directly to obtain information or their consent. Where there is concern about the safety of a conviction, it is, however, vital that the CCRC can thoroughly investigate. Without the power to access this data the CCRC would not have the tools it needs to do its job and miscarriages of justice may go unnoticed and uncorrected.

Case study 1:

Case/Investigation name: Mr K

Communications data required: Telephone service use (billing) data (outgoing calls).

Background/Reason for requesting data: Mr K was convicted of rape. An issue in the case related to alleged telephone calls between him and the complainant. The CCRC wished to investigate the existence and duration of these calls.

Outcome: The CCRC obtained communications (billing) data relating to Mr K's phone which had not been obtained during the police investigation. This data supported his defence at trial and raised concerns about the credibility of the complainant. The CCRC decided to refer this case to the Court of Appeal on the basis of this data and related arguments.

Would the outcome have been achieved without the data: The CCRC would not have been able to fully investigate or refer this case without the data. Whilst Mr K's phone bill(s) also contained the relevant information, the CCRC needed to ensure that the information provided was genuine and accurate. Being able to access the data directly from the communications service provider enabled the CCRC to make the appropriate checks before deciding to send this case back to the Court.

Case study 2:

Case/Investigation name: Mr J

Communications data required: Incoming call data.

Background/Reason for requesting data: The CCRC was informed that a person purporting to be a witness from a trial had been making telephone calls offering to retract their evidence in exchange for money. The CCRC wished to investigate this issue and whether it affected the safety of the conviction(s).

Outcome: The CCRC used its powers to obtain communications data which enabled it to identify the call(s) in question and the telephone number from which they had been made. This enabled the CCRC to make further enquiries in order to ultimately identify who had made the calls.

Would the outcome have been achieved without the data: In the circumstances this was the only way for the Commission to seek to identify who had made the calls. Without access to communications data, the CCRC would not have been able to properly investigate this issue.

Case study 3: Hypothetical

Case/Investigation name: Mr Z

Communications data required: Internet connection records.

Background/Reason for requesting data: The Court of Appeal directed the CCRC to conduct an investigation into whether a juror had undertaken internet and/or social media research into a defendant. The Court of Appeal takes misconduct (including "research") by jurors very seriously and it can lead to convictions being quashed.

Outcome: This investigation was limited to interviewing the juror in question; however a similar case could be assisted by being able to demonstrate that a particular device had accessed a website (e.g. a search engine, social media website, specific news outlet etc) or when such access had taken place (e.g. when the jury were in deliberations).

Would the outcome have been achieved without the data: Without access to internet connection records, the CCRC would be unable to undertake an investigation of this nature. Being unable to investigate fully could lead to a potentially unsafe conviction not being corrected.

Department for the Economy in Northern Ireland

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Department for the Economy in Northern Ireland
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014 (as Department for Enterprise Trade & Investment in Northern Ireland)
• Applications: 28 • Notices & authorisations: 167

Requirement to be able to acquire communications data

In Northern Ireland, the Department for the Economy are able to acquire communications data because in Northern Ireland they have responsibility for investigating trading standards offences.

Case study 1:

Case/Investigation name: Mr D

Communications data required: Telephone subscriber details to identify trader.

Background/Reason for requesting data: A trader offering domestic appliance repair services was using upwards of 15 trading names and multiple mobile telephone numbers in advertisements in local newspapers. The trader went to consumers' homes and obtained cash to pay for parts needed to effect repairs, but failed to return to carry out the necessary work.

Outcome: Communications data allowed the tracing of the phone numbers back to a common user and as a result he was convicted under the Theft Act (Northern Ireland) 1969 and sentenced to six months imprisonment suspended for two years.

Would the outcome have been achieved without the data: Without access to this trader's communications data it would not have been possible to identify the specific individual responsible.

Case study 2:

Case/Investigation name: Mr R

Communications data required: Subscriber details

Background/Reason for requesting data: Two elderly consumers (one over 90) employed a trader to carry out plastering work at their homes. Both paid the trader large sums of money in advance. The trader commenced the work but left the jobs needing a considerable amount of work still to be done. The trader could only be traced through his mobile phone number.

Outcome: Communications data allowed the trader to be identified and he was subsequently convicted of offences under the Fraud Act 2006 and the Consumer Protection from Unfair Trading Regulations 2008. He was fined £1,050 and given a 16 month prison sentence suspended for 2 years. The court ordered him to pay £2,000 compensation to the consumers.

Would the outcome have been achieved without the data: Without access to the **c**ommunications data it would not have been possible to identify this individual.

Case study 3:

Case/Investigation name: Mr P

Communications data required: Identifying the specific user of an IP address.

Background/Reason for requesting data: Trader was selling counterfeit t-shirts via online sites.

Outcome: The communications data for the IP addresses used to place the advertisements made it possible to establish the trader's identity and address. A subsequent operation resulted in the seizure of equipment for producing counterfeit garments. Trader was successfully prosecuted under the Trade Marks Act 1994. There is an on-going case to recover criminal assets in the region of £400,000.

Would the outcome have been achieved without the data: It would not have been possible to identify this trader without access to his communications data.

Case study 4:

Case/Investigation name: Mr B

Communications data required: Identifying the specific user of an IP address

Background/Reason for requesting data: A rogue car trader obscured his identity by using various "pay as you go" mobile phones to try and hide his connection to numerous car adverts on different websites. Through obtaining details of the IP

address used to access various websites, the Trading Standards Service was able to identify the trader as the person uploading the adverts together with his geographic address.

Outcome: The trader was found guilty of 10 charges under the Consumer Protection from Unfair Trading Regulations 2008. He was fined £5,000 and ordered to pay £1,000 compensation to the victim.

Would the outcome have been achieved without the data: As the trader was masquerading as a private seller and had no trading premises, without the access to his communications data it would not have been possible to connect him to the cars being offered for sale.

Department of Health

The Medicines and Healthcare Products Regulatory Agency

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• The Medicines and Healthcare Products Regulatory Agency under 'the Department for Health' entry
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder • (d) in the interests of public safety • (e) for the purpose of protecting public health
Communications data applications covering the period from January to December 2014
• Applications: 61 • Notices & authorisations: 102

Requirement to be able to acquire communications data

The Medicines and Healthcare Products Regulatory Agency (MHRA) is part of the Department of Health and is the principal law enforcement agency with responsibility for investigating criminal acts relating to medical products. The Agency enforces the provisions of the Human Medicines Regulations 2012, the 1968 Medicines Act, the Blood Safety and Quality Regulations 2004, the Good Laboratory Practice Regulations 2005 and the Health Ministers and Medical Devices Regulations 2003.

Communications data is used in investigating serious crimes, such as counterfeiting medicines. For example, communications data can demonstrate links between conspirators.

Almost all criminal investigations carried out by the MHRA require access to communications data. Approximately 75 to 80 per cent of cases are internet based, in which the use of domain names, telephone numbers, email addresses, social media and other means of communication are key to the business of these organised crime groups involved in the sale and supply of illegally traded and counterfeit / falsified medical products. The techniques used by the agency include the use of covert human intelligence sources, covert internet investigators and test purchase officers. Detailed communications data is required to support these proactive investigations

Case Study 1

Case/Investigation name: Operation SINGAPORE

Communications data required: Telephone subscriber and e-mail details of over 20 individuals were requested.

Reason for requesting: In an investigation into counterfeit medicines in the UK supply chain, telephones were retrieved during searches but the main suspect 'A' became aware of the investigation and disposed of his telephones in advance. In addition it was known that 'A' was impersonating a number of individuals, as he was known by reputation and companies would not deal with him. Subscriber details were used to place 'A' making calls and arranging meetings when impersonating individuals in order to buy equipment used in the manufacture of counterfeit medicines. 'A' was arranging for packaging, materials, shipments and deliveries. Call data linked 'A' to all the steps in the supply of the counterfeit medicines.

The telephone subscriber details were also required to prove 'A' was the person that co-conspirators were ringing.

Outcome: The main suspect was sentenced, after a 4 month Crown Court trial, to 8 years imprisonment for counterfeiting medicines following a 3 year investigation involving 13 countries, 93 witnesses, 17,000 pages of evidence, 4,000 exhibits and 2.1 million doses of counterfeit versions of potentially life-saving medicines.

Would the outcome have been achieved without the data: Analysis of call data could link 'A' to periods of activity when arrangements were being made to have packing falsified, to collect cargo shipments from airports in Europe and arrange shipping. The ability to access this level of data was essential to the successful prosecution and the ability of the agency to protect public health and save lives.

Case Study 2

Case/Investigation name: Operations Howard, Red Rock and Poodle

Communications data required: Telephone subscriber checks. Analysis revealed over 50 text messages detailing instructions and parcels sent from India as well as outgoing text messages from the UK suspect detailing payment of money into several bank accounts relating to the sale of counterfeit and unlicensed medicines. The sender of the incoming texts was an Indian National based in Bombay/Mumbai.

Reason for requesting: As part of an MHRA Enforcement Group's investigations (Operation HOWARD), into possible breaches of The Human Medicines Regulations 2012, several mobile phones were seized at the scene of arrest of a UK suspect. Forensic examination revealed telephone numbers and text messages to and from suspects. The text messages contained instructions between the parties on what

medicines were being imported into the UK, and what payments were being sent out. Analysis revealed two Indian telephone numbers of particular interest

Outcome: Developed intelligence from the communications data identified two UK major “Drop Shippers” willing to sell and supply unlicensed medicinal products in commercial quantities direct to the public. A covert investigation commenced and led to the apprehension of the major suspects behind two international criminal networks. Over 10 million doses of unlicensed medicines, cash and other property were seized. The cost of these medicines is valued at over £6.5 million.

Would the outcome have been achieved without the data? All these cases were intelligence led and built from communications data throughout the investigations. The communications data obtained subsequent to the warrant and arrests built a picture of a conspiracy between the suspects.

Case Study 3

Case/Investigation name: Operation Peace

Communications data required: Telephone Subscriber details. Analysis of this data identified the sales activity of the main suspect and identified his contacts and activities.

Reason for requesting: A telephone was retrieved during an inspection where 11,000 unlicensed medicines, used to treat erectile dysfunction, were seized. The telephone subscriber details were required to prove the telephone belonged to the suspect at the address.

Outcome: The suspect admitted the offences based on the strength of evidence obtained using communications data. This has resulted in an early guilty plea, saving a lengthy trial. Communications data from the initial telephone have revealed the telephone numbers of at least five other people involved in the wholesale supply of unlicensed medicines and also hundreds of purchasers.

Further requests for communications data will be necessary to identify the subscribers of the new telephone numbers which will support follow on investigations into further suppliers of unlicensed medicines.

Would the outcome have been achieved without the data: It would not have been possible to progress the enquiry without the data and this is the only method of evidentially identifying the subscriber of a telephone and thus using the information in court.

Case Study 4

Case/Investigation name: Operation Fitzroy

Communications data required: Subscriber details for two mobile telephone numbers

Reason for requesting: Parcels containing counterfeit Cialis (a prescription medicine) were intercepted en-route to an address in London. Intelligence checks showed 'A' registered as the council tax payer of the address. However, further checks showed a student of the same name living in Loughborough. Around the same time, parcels from the same supplier in India started being addressed to 'B' at 2 addresses in Loughborough. Warrants of entry were obtained and all three addresses visited simultaneously. In total, seizures at the addresses and at postal hubs resulted in the seizure of 180,547 counterfeit and generic products representing a monetary value of £610,000. 'A' was arrested at the London address and a third subject 'C' was arrested at the Loughborough address. Telephone numbers found at two addresses and subsequent communications data analysis were used to link the two individuals together and to rule out the student (subject 'B') as being involved. The subscriber details obtained have now linked a further suspect and a further prosecution is pending.

Outcome: Both subjects eventually pleaded guilty at Crown Court. On 5th July 2013 'A' was sentenced to 8 months imprisonment suspended for 2 years and to perform 140 hours unpaid work. **'**C' was sentenced to 12 months imprisonment suspended for 2 years and to perform 200 hours unpaid work.

Would the outcome have been achieved without the data: It would not have been possible to link the 2 subjects to the offences or to link the further subject whose prosecution is pending.

Anti-Fraud Unit

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• The Anti-Fraud Unit under 'the Department for Health' entry
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• The Anti-Fraud Unit have not previously had a specified designated senior officer

In November 2014 the Department of Health set up an Anti-Fraud Unit (DH AFU) to tackle crime against the Department and its Arm's Length Bodies (ALBs)[7]. DH AFU is also the departmental sponsor for the anti-crime function within the NHS Business Services Authority (NHSBSA). DH AFU investigates allegations of fraud and corruption which do not affect the health service or relate to the health service but are nevertheless cases of very significant ministerial, government or public interest and require action to be taken in the name of the Secretary of State, or carry a risk of significant reputational damage to the Department or its ALBs. Investigators have powers under the National Health Service Act 2006 to prevent, detect and investigate offences and other unlawful activities carried out against the health service.

The Investigatory Powers Bill provides a designated senior officer in the DH AFU, as well as in MHRA. Under RIPA, only the MHRA had a designated senior officer. DH AFU is a new unit with a distinct remit which does not duplicate that of MHRA nor NHS Business Service Authority (who are also able to acquire communications data). In future, as DH AFU's caseload increases, access to communications data will be needed in order to conduct effective criminal investigations.

DH AFU fraud investigations will depend on communications data to identify suspects, link co-conspirators and establish the mechanics of the offences committed. The case studies provided show the hypothetical impact of these powers in the context of real cases.

Case study 1:

Case/Investigation name: NUFFIELD.

Communications data required: Mobile phone subscriber and billing data.

Background/Reason for requesting data: In NUFFIELD the investigation involved a conspiracy to defraud the NHS (via diversion of DH bank account funds to a number of external co-conspirator accounts) costing the Department in excess of £1million.

Outcome: The use of communications data in this investigation would have been instrumental in demonstrating the range and depth of conspiracy between subjects, using registration and billing data across mobile devices to evidence the level and timing of communication taking place prior to diversion and transference of moneys across a range of bank accounts. Access to communications data may have demonstrated that on the specific days payments were made into bank accounts, contact was made between the recipients, as well as contact being made with the suspected money launderers on the days when monies were transferred into their accounts.

[7] Details of Department of Health ALBs are published at: https://www.gov.uk/government/publications/how-to-contact-department-of-health-arms-length-bodies/department-of-healths-agencies-and-partner-organisations

Would the outcome have been achieved without the data: Using communications data could have brought a quicker resolution to this investigation and a more effective outcome. Access to communications data could have resulted in sufficient evidence being gathered to secure additional charges relating to conspiracy and money laundering.

Case Study 2:

Case/Investigation name: KENNET

Communications data required: IP addresses, email ownership

Background/Reason for requesting data: This investigation involves the impersonation of the NHS Patient Safety Alert system and NHS officials Access to communications data would have proved useful to establish ownership of internet domains and email addresses in order to identify suspects.

Outcome: The NHS Patient Safety Alert is managed by NHS Improvement, a DH ALB, which means that the investigation falls within the remit of DH AFU. The case carries a high reputational risk which in order to attach the appropriate priority and resources to the investigation should be investigated within the department in order to find a quick resolution. Without access to communication data, the investigation may be delayed which could affect a potential prosecution.

Would the outcome have been achieved without the data: Without access to communications data, a complete investigation could not be pursued. The unavailability of data means that suspects cannot be identified and the perpetrators may continue to undermine the Patient Safety Alert system and impersonate NHS officials.

Department for Transport

Accident Investigation Branches

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Marine Accident Investigation Branch • Air Accident Investigation Branch • Rail Accident Investigation Branch
Statutory purposes under clause 58(7) available to these authorities
• (d) in the interests of public safety
Communications data applications covering the period from January to December 2014
Marine Accident Investigation Branch: • Applications: 1 • Notices & authorisations: 1 Air Accident Investigation Branch: • Applications: 6 • Notices & authorisations: 10 Rail Accident Investigation Branch: • Applications: 2 • Notices & authorisations: 2

Requirement to be able to acquire communications data

Department for Transport (DFT) Accident Investigation Branches (Air (AAIB), Marine (MAIB) and Rail (RAIB)) use communications data in investigations into accidents. Their uses of communications data are varied, but principally revolve around the understanding of events immediately before and after accidents. For example, if a flight crashes the investigation branches may need to determine if the pilot was using a mobile phone at the time of the crash.

The following case studies provide examples of how communications data has been used. Access to communications data is crucial to the work of the AIBs. While they do not use the powers very often, when they do it is because it is the only way to obtain the necessary information. The loss of those powers will sometimes have a direct impact on the AIBs ability to conduct meaningful investigations, improve transport safety and therefore save lives in future.

DFT MAIB case study 1:

Case/Investigation name: Loss of the yacht *Cheeki Rafiki* and its four crew while crossing the Atlantic on 16 May 2014.

Communications data required: Subscriber information; traffic data; service use information.

Background/Reason for requesting data: The UK registered yacht *Cheeki Rafiki* had sailed from Antigua on 4 May 2014 to make passage across the Atlantic to return to Southampton. Twelve days later the yacht capsized in heavy weather approximately 720 miles east-south-east of Nova Scotia, Canada. Despite an extensive air search that found the upturned hull of the yacht, the four crew remain missing.

Outcome: The only available information about the vessel's movements and the communications of the crew was contained in communications data. Specifically:

- Each time *Cheeki Rafiki*'s satellite telephone connected to the network a record was made of the vessel's position. Analysis of this data allowed investigators to accurately reconstruct the vessel's track up until close to the time of its loss and to map it against the prevailing wind and wave data to reconstruct the forces on the yacht. This information was crucial to understanding how the yacht's structure deteriorated until it failed.
- Connection times and telephone records enabled investigators to pursue enquiries leading to a full understanding both of the yacht's deteriorating condition and the advice the skipper received from the principal of the company managing the yacht.

Would the outcome have been achieved without the data: No. Communications data was pivotal to the investigation. Without it, the investigation would not have uncovered sufficient evidence to reconstruct the events leading to the accident, draw meaningful conclusions, or make substantial recommendations. As a result of this investigation, wide ranging recommendations were made concerning the inspection and repair of yachts whose manufacture involved bonding a strengthening matrix into the hull.

DFT AAIB case study 1:

Case/Investigation name: G-CRST, Agusta 109E, 16 January 2013, in central London

Communications data required: Mobile phone traffic data

Background/Reason for requesting data: At 07:59 on Wednesday 16 January 2013 a public transport helicopter collided with a construction crane engaged in a high-rise building project in central London. The pilot and a pedestrian on the street below were fatally injured and several other pedestrians were seriously injured. The AAIB, police and emergency services were involved but it soon became apparent

that the accident was not a ‘scene of crime’ and the police agreed that primacy for the investigation would rest with the AAIB.

Evidence from third parties suggested that the pilot was using the text facilities on his mobile telephone during the flight. The progress of the flight, prior to the accident, was recorded on radar but it was essential for the AAIB to synchronise this with the use of the mobile phone to fully determine the activities of the pilot prior to his death.

Outcome: Mobile communications data obtained by the AAIB proved to be fundamental in the investigation.

Would the outcome have been achieved without the data: No. Had the data not been obtained, the investigation would have been incomplete, a significant safety issue would not have been identified and the AAIB would have failed in its legal duty to investigate fully the causes of an accident.

DFT RAIB case study 1:

Case/Investigation name: Passenger trapped and dragged in the closed door of a train departing from Hayes & Harlington station.

Communications data required: Mobile telephone call records of train driver.

Background/Reason for requesting data: At around 13:10 hrs on Saturday 25 July 2015, a passenger was dragged along the platform at Hayes & Harlington station, London, when the 11:37 hrs service from Oxford to London Paddington departed while her hand was trapped in a door. The train driver did not identify that the passenger was trapped and the train moved off. The passenger was dragged for about 19 metres and suffered head, hand and back injuries.

Responsibility for dispatching trains safely at Hayes & Harlington station resides with the driver, who controls the train doors and is expected to make a final check that it is safe to depart before doing so. The RAIB was keen to understand whether the driver had been distracted from performing his duties safely.

Outcome: Communications data indicated that the train driver had been using his mobile phone while travelling between two stations and while stationary at another in the minutes leading up to the accident. The RAIB considered this to be such a serious breach of the railway rule book that it immediately provided the driver’s employer with information about his use of the phone while driving. This enabled the employer to take appropriate action, and the safety consequences of train drivers using phones while driving has been highlighted in the RAIB’s investigation report.

Would the outcome have been achieved without the data: No. The RAIB’s access to mobile communications data revealed a major safety concern about which the industry would otherwise have been completely unaware. The industry has no means of monitoring misuse of mobile telephones by train drivers, particularly when personal phones are used.

The Maritime and Coastguard Agency

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• The Maritime and Coastguard Agency
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder • (d) in the interests of public safety • (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health
Communications data applications covering the period from January to December 2014
• Applications: 3 • Notices & authorisations: 3

Requirement to be able to acquire communications data

The Maritime and Coastguard Agency (MCA) acquire communications data very rarely but when they do it is likely to be in threat to life situations, for example to locate someone lost at sea.

DFT MCA case study 1 - HM Coastguard

Case/Investigation name: Missing Person West Wales

Communications data required: Location Information

Background/Reason for requesting data: A person was reported missing in West Wales and was believed to be suicidal. Coastguard units were mobilised to search a large area of dangerous cliff terrain at night. During the initial search the person called home on several occasions.

Outcome: His position was determined by the use of communications data, specifically the particular cell he was connected to.

Would the outcome have been achieved without the data: This reduced a potential 12 hour search to less than one hour, and the person was subsequently found and protected from further harm.

DFT MCA case study 2 - MCA Enforcement Unit

Case/Investigation name: R v Fairless

Communications data required: Subscriber details

Background/Reason for requesting data: A fisherman from St Austell, Cornwall used a fax machine in a local hotel to send forged statutory seafarer documents to the MCA – such documents, for example, allow the temporary admission of seafarers into foreign territory. Communications data proved the offence by identifying the hotel, and when the fax was sent. The fisherman was a regular in the hotel and supplied them with shellfish.

Outcome: He was successfully prosecuted for fraud and received a fine totalling £14,000.

Would the outcome have been achieved without the data: No. Furthermore, although fax machines are used less frequently, smart phones are now commonly used for some of the tasks that fax machines did previously. If the IP address of the phone was available, the MCA may have been able to show it logging onto the public Wi-Fi in the hotel at the relevant time, or indeed sending the forged documents directly from the phone.

Department for Work and Pensions

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Fraud and Error Services • Child Maintenance Group
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
Child Maintenance Group: • Applications: 21 • Notices & authorisations: 30 Fraud and Error Services: • Figures are not available for Fraud and Error Services because, as explained below, they currently acquire communications data under the Social Security Administration Act 1992

Requirement to be able to acquire communications data

Department for Work and Pensions (DWP) Fraud and Error Service (FES) currently uses powers under Section 109 of the Social Security Administration Act 1992 to obtain communications data in order to support its functions of detecting, prosecuting and preventing social security benefit offences. This provision was introduced as part of the Social Security Fraud Act 2001 (SSFA). The Investigatory Powers Bill revokes the powers to acquire communications data in the SSFA in order to ensure that all applications for communications data by DWP are subject to the robust safeguards in the Bill.

Although only one part of the wide range of information that FES can obtain, communications data is instrumental and can provide vital investigative leads that would not otherwise come to light. For example, a person may be fraudulently claiming benefits as a single person but communications data links a partner to the same address as the claimant. Communications data can often be used to identify serious and organised attacks on the benefits system, in many cases attacks made by organised crime groups and ‘faceless’ individuals.

The Child Maintenance Group (CMG) has responsibility for the calculation and collection of child maintenance. Communications data is used to investigate fraud against the child maintenance system, including bogus second applications to reduce liability, claiming to be outside the jurisdiction of the scheme and conspiracy

with others to obtain a negative paternity result. For example, communications data can be used to identify the address of the fraudulent applicant.

Case study 1:

Case/Investigation name: Operation Mindar

Communications data required: Telephony data

Background/Reason for requesting data: This is a human trafficking and benefit fraud investigation. The same mobile number was linked to a number of national insurance numbers and potentially fraudulent benefit claims. This telephone number enabled DWP to identify the main subject of the investigation.

Outcome: The subject was identified and it was subsequently determined that he was wanted for serious offences in Romania. He was deported to face justice for those offences. An additional outcome has been 40 individuals, including many children, being freed from a life of slavery and servitude.

Would the outcome have been achieved without the data: No. If the telephone data had not been available an essential tool in the evidential chain would have been lost. Access to this data supported DWP (and is continuing to provide evidence) in identifying the total criminality associated with this case.

Case study 2:

Case/Investigation name: Operation Boromo

Communications data required: IP address data

Background/Reason for requesting data: This was a DWP led, multi-agency investigation of an organised attack on the UK immigration and welfare systems by an organised crime group.

Outcome: Over 1,500 tax credit claims were identified with a total overpayment calculated at over £11million with a further £17m of loss prevented. As these fraudulent claims were submitted online, DWP were able to identify the primary perpetrators by resolving the IP addresses used to commit the crimes. Six members of the organised crime group are on remand, charged with general conspiracy to defraud Government departments.

Would the outcome have been achieved without the data: Without this data it is doubtful the operation would have been such a success. Communications data allowed previously unknown members of the organised crime group to be identified, helping to provide evidence of the scale of the fraud.

Case study 3:

Case/Investigation name: Child maintenance fraud

Communications data required: IP address data and service use data

Background/Reason for requesting data: ‘A’ was a non-resident parent in a Child Maintenance Case. He alleged that he resided in Ireland, rather than the UK. This placed him beyond CMG’s jurisdiction and not liable to pay child maintenance. During an investigation CMG became aware of phone calls and emails sent and made by ‘A’ to his children and their grandmother. An application under RIPA was made to the communications service providers, which showed the calls were made from within the UK and the originating IP address was traced to a company based in the UK and to a property in the UK, which ‘A’ had bought. He was arrested and interviewed where he fully admitted his guilt.

Outcome: ‘A’ was convicted of two counts of fraud and sentenced to 12 months imprisonment. CMG were able to recover £20,000 in unpaid maintenance.

Would the outcome have been achieved without the data: No. The acquisition of the IP address and the service use data established ‘A’ was not in Ireland and that he was working for his brothers company in the UK.

Financial Conduct Authority

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Financial Conduct Authority
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder • (j) for the purpose of exercising functions relating to— (i) the regulation of financial services and markets, or (ii) financial stability
Communications data applications covering the period from January to December 2014
• Applications: 224 • Notices & authorisations: 3,768

Requirement to be able to acquire communications data

The Financial Conduct Authority (FCA) has civil and criminal powers under the Financial Services and Markets Act 2000 to investigate issues such as insider dealing and market manipulation. In such cases, being able to demonstrate communications between suspects is essential. The FCA are the most frequent user of communications data of any of the authorities in this document.

Case study 1:

Case/Investigation name: Operation COTTON

Communications data required: The investigation team submitted 63 applications in total relating to numerous types of communications data, including IP addresses.

Background/Reason for requesting data: Operation COTTON was an investigation into a sophisticated boiler room operation (where fraudsters cold-call investors offering them often worthless, overpriced or even non-existent shares) which shifted locations on a regular basis. The boiler room employed 25-30 staff at any one time to cold-call prospective investors including the elderly and vulnerable, resulting in those running the boiler room amassing criminal proceeds totalling nearly £5m. During the investigation, 63 RIPA applications were made and approved. The resultant data from some of these applications supported victims' accounts of how they had been contacted and defrauded. In addition, IP data was used to identify the location of the new offices of the fraudsters, at which search warrants were executed, phones and computers seized and persons arrested.

Outcome: Eight defendants were sentenced to a total of 34 years' imprisonment, and criminal assets in excess of £1m are the subject of confiscation proceedings.

Would the outcome have been achieved without the data: No. Communications data was essential to the following outcomes:

- Locating the new offices and preventing further vulnerable consumers being defrauded;
- Executing search warrants, seizing key evidence and enacting confiscation proceedings.

Case study 2:

Case/Investigation name: Operation TABERNULA

Communications data required: The investigation team submitted numerous applications relating to subscriber information, traffic, service use and IP data.

Background/Reason for requesting data: Operation Tabernula was the FCA's largest and most complex insider dealing investigation. It concluded with the conviction of two individuals on 9 May 2016, three other individuals having pleaded guilty in 2013 and 2014. The sentences imposed ranged from 19 months' imprisonment to four and a half years' imprisonment. The offending in this case was highly sophisticated and took place over a number of years. The defendants put in place elaborate strategies designed to prevent the authorities from uncovering their activities. These included the use of unregistered mobile phones, encoded and encrypted records, safety deposit boxes and the transfer of benefit using cash and payments in kind. Investigators, forensic accountants, lawyers, markets experts, intelligence analysts and digital forensic specialists pooled their skills to unravel the conspiracy. This was achieved through painstaking analysis of more than 200,000 lines of trading data, over 500,000 phone communications and more than 10 million emails, instant messages and individual digital items.

Outcome: Two suspects were found guilty of conspiracy to commit insider dealing following a trial and three suspects pleaded guilty to insider dealing.

- Paul Milsom: 2 years imprisonment and £245,000 confiscation order;
- Graeme Shelley: 2 years imprisonment sentence suspended and £588,000 confiscation order;
- Julian Rifat: 19 months imprisonment, fined £100,000 with £159,402 costs order;
- Andrew Hind: 3.5 years imprisonment and benefit to be determined; and
- Martyn Dodgson: 4.5 years imprisonment and benefit to be determined

Would the outcome have been achieved without the data: No. Communications data was essential to the following outcomes:

- Confirming associations between main targets (trader with middleman and middleman with insider);
- Attributing pay as you go phones;
- Confirming face to face meetings between targets;
- Identifying new targets (middleman and insider);
- Accurate housing of targets in advance of search and arrest phases.

Case study 3:

Case/Investigation name: Operation HOWDEN

Communications data required: The investigation team submitted 9 applications relating to numerous types of communications data, including IP addresses.

Background/Reason for requesting data: Operation Howden was an FCA investigation into insider dealing by an individual in a position of trust at a FTSE-listed company. FCA Cyber Forensics worked with a trading broker to assess how the suspect was placing trades electronically. This work identified that the trades placed were made via a mobile digital device and were being executed via the broker's app. It was established that the majority of the instructions to trade were made via IP addresses attributed to the suspect's place of work, their residential address and a hotel, which through financial investigation they were confirmed to have stayed at during the relevant dates. Reviewing the browser strings passed through the app also identified that the device used to place some of the trades was an iPad – this knowledge assisted the search team during the arrest phase of the operation.

Outcome: The suspect pleaded guilty to 2 counts of insider dealing and was sentenced to 12 months imprisonment. The benefit to the perpetrator from this criminal conduct was assessed by the FCA as being £203,234 and a Proceeds of Crime Act 2002 confiscation order was granted for this full amount.

Would the outcome have been achieved without the data: No. Communications data was essential to the following outcomes:

- Identifying devices and locations where suspicious trades were placed to commit the crime alleged at the time;
- Directing search and seizure action in relation to searches of premises and the arrest of certain individuals;
- Demonstrating an overwhelming case through the evidence amassed which resulted in a guilty plea.

Case study 4:

Case/Investigation name: Operation ALDERSHOT

Communications data required: The investigation team submitted 17 applications in total requesting 18 services relating to subscriber information, 30 relating to traffic data and 7 relating to service use data.

Background/Reason for requesting data: Operation ALDERSHOT was an investigation into insider dealing, which originated from a larger insider dealing ring case, Operation Tabernula, and featured criminal activity between two suspects engaged in insider dealing. This case relied on access to communications data to help investigators build detailed chronologies and patterns of activity. Chronologies were built using relevant case information and data – calls, texts, emails, trading records, call recordings and deal documentation. As part of the investigation, communications data covering 4 years and 700,000+ lines of data were reviewed.

Outcome: Following guilty pleas, one suspect was sentenced to 2 years' imprisonment and the other suspect to a suspended sentence of 2 years' imprisonment; their criminal assets amounted to £800,000. The suspended sentence was imposed directly as a result of significant assistance provided to the prosecution by one of the defendants against the other. In the case of both defendants, the communications evidence was key to obtaining guilty pleas and the attendant saving in time and costs to the prosecution and to the court system.

Would the outcome have been achieved without the data: No. Communications data was essential to the following outcomes:

- Attributing pay as you go phones;
- Creating a condemning chronology of events;
- Identifying specific devices containing evidence of timely interactions.

Fire and rescue authorities

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• A fire and rescue authority under the Fire and Rescue Services Act 2004 • Northern Ireland Fire and Rescue Service Board
Statutory purposes under clause 58(7) available to these authorities
• (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health
Communications data applications covering the period from January to December 2014
• Applications: 0 • Notices & authorisations: 0

Requirement to be able to acquire communications data

The fire and rescue services may need to acquire communications data in an emergency to prevent death or injury.

Sometimes people get disconnected when contacting the emergency services. This could be for a number of reasons such as low battery, poor signal or a phone being damaged or taken as part of an incident. There will also be circumstances where a person in difficulty may be unable to describe their location with sufficient accuracy for the emergency services to locate them. Communications data can be used to assist the emergency services getting to a person in time.

In practice, the fire and rescue services very rarely acquire communications data under the Regulation of Investigatory Powers Act 2000 (RIPA) and that is likely to continue to be the case under the Investigatory Powers Bill. This is because the Communications Act 2003 requires certain communications service providers to provide communications data to the emergency services following an emergency call made to 999 and 112 emergency numbers. There is a period of one hour after the termination of an emergency call in which access to the data for the emergency services falls outside the provisions in RIPA and in the Bill. The fire and rescue services have been provided powers in this Bill in case they need to acquire communications data in an emergency outside of these circumstances.

Food Standards Agency

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Food Standards Agency • Food Standards Scotland
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• These authorities are not currently able to acquire communications data

Requirement to be able to acquire communications data

The National Food Crime Unit (NFCU) was established by the Food Standards Agency (FSA) in December 2014 as part of the government response to recommendations made by the Elliott Review into the integrity and assurance of food supply networks. Professor Elliott's review was a response to the 2013 horsemeat scandal. The remit of the NFCU is to tackle serious food fraud and as such is a new requirement with an overarching national remit to tackle serious or complex food crime within food supply networks. This new requirement brings with it a necessity to access communications data. The Government previously removed the ability of the Food Standards Agency to acquire communications data because the power had not been used. However, the establishment of the NFCU since then has brought with it a need to gather intelligence on serious crime so the Government has decided to return the powers to the FSA. Access to communications data is essential for food crime investigations because it can help to identify offenders and demonstrate links between individuals involved in fraudulent food supply chains.

As the NFCU has only recently been established, there are few operational case studies to demonstrate the requirement for communications data. However, the below examples illustrate the circumstances in which the NFCU may need to acquire communications data.

Case study 1:

Case/Investigation name: Operation SYCAMORE

Communications data required: IP addresses, subscriber data

Background/Reason for requesting data: Op Sycamore is the National Food Crime Unit's response to at least 6 deaths in the UK (the figure could be higher) in the last 18 months from persons consuming 2,4 dinitrophenol, commonly known as DNP, including the well-publicised death of Eloise Parry in April 2015 from DNP toxicity. DNP is a chemical which is unsafe for human consumption but is taken by those seeking to lose weight or improve muscle definition. It is therefore popular within the body building and fitness communities and individuals wishing to lose weight quickly and/or those suffering with body dysmorphia or eating disorders. DNP is illegal to sell for human consumption. It is not a medicine or pharmaceutical product and so does not come under the remit of the Medicines and Healthcare Products Regulatory Agency.

The NFCU identifies websites through which DNP is marketed and sold. Although these sites often quote disclaimers that the product is "not for human consumption" or for "research purposes only" the narrative is accompanied by images and text which is intended to lead the consumer to conclude that the substance is suitable for ingestion.

Often the websites will contain email addresses for customer contact and it is the NFCU's intent to pursue those individuals behind the sale of DNP by having access to IP addresses to identify those behind the websites and from where they are being operated in order to take action against them. When operational interventions take place against suspects identified in this way, communications data would also be used to identify others involved in the distribution of DNP and to identify vulnerable people who may be consuming the toxic substances.

Would the outcome have been achieved without the data: Currently NFCU activity is restricted to sending Abuse Complaints to the internet domain registry in order to have the website removed (with varying levels of success). The ability to access communications data would allow the NFCU to identify the individuals behind these websites and potentially take further action.

The NFCU is currently building its e-Crime capabilities to ensure it can tackle the growing problem of fraudulent and harmful food products sold online. Failure to gain access to communications data would severely hamper the effectiveness of this capability as it would not be possible to identify those behind criminal websites.

Case study 2:

Case/Investigation name: Op THAMES and MARINO 2.

Communications data required: Billing and subscriber data

Background/Reason for requesting data: Operation Thames and Marino 2 are multi-agency investigations into the supply of illicit meat and meat products that pose a serious risk to human health. The suspects operate outside of the normal regulatory domain for food business operators. Communications data would be extremely valuable to the inquiry, since it would enable the NFCU to demonstrate association between suspects; evidence the scale, timeframe and nature of the

illegal activity; and identify individuals and food businesses involved in the onward distribution of the products.

Would the outcome have been achieved without the data: Access to communications data would substantiate some of the links that are currently unconfirmed between the identified suspects, including the complex supply routes. It would also provide an invaluable route for intelligence gathering to correlate with existing data and to complement – or to negate the need for – other surveillance. The development and progression of this intelligence package is hampered without access to communications data.

Case study 3:

Case/Investigation name: European Distribution Fraud

Communications data required: Subscriber, billing data and IP addresses.

Background/Reason for requesting data: European Distribution Fraud (EDF) is a widespread issue affecting many types of business and products, including electrical goods, alcohol and food. In general terms a criminal posing as a well-known and reputable UK company will contact a supplier and place an order. The goods or products are despatched or collected but never paid for leading to substantial losses for the supplier company. Often they only realise they have been a victim of fraud when they contact the genuine company for payment to be told that they placed no such order.

Often the order will be placed via email using a domain name similar to the genuine company's, whilst logos, websites and contact details may all be cloned. Sometimes the fraudster may use a recently acquired company and place several small orders to build up credibility and trust before a much larger order is stolen.
The NFCU is aware of several occasions where genuine UK food suppliers have had orders placed and then stolen, leading to a loss of tens of thousands of pounds. Where food stuffs are stolen it is suspected that a significant health and food safety risk is also involved whereby food is transported in unhygienic vehicles or stored in unsatisfactory conditions.

Would the outcome have been achieved without the data: The NFCU is keen to tackle this area of food crime which falls squarely within its area of responsibility. The absence of access to communications data means that the unit cannot currently provide any meaningful response. It is suspected that those perpetrating such crimes will target a specific business and seek the maximum order value from them before moving on to new victims. Often contact will be by mobile phone and email and so communications data is vital to establish links between those who are acting in the fraud and those organising it in order to identify the wider aspects of the operation and to link all subjects.

Gambling Commission

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Gambling Commission
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• Applications: 8 • Notices & authorisations: 12

Requirement to be able to acquire communications data

The Gambling Commission are responsible for investigating and prosecuting offences under the Gambling Act 2005. For example, the Commission investigates unlicensed bookmakers who provide illegal gambling services and conducts investigations into the manipulation of betting associated with sporting events (match fixing). The Commission investigates illegal gambling being provided remotely over the internet targeting British consumers.

Since the implementation of the Gambling (Licensing and Advertising) Act 2014 on the 1st November 2014, the Commission has licensed the entire UK facing online gambling market. The total gross gambling yield of this sector was £3.6bn, representing a 29 per cent share of the £12.6bn licensed industry. The Commission has received over 590 reports of and tackled 109 incidents involving illegal gambling remotely targeting British consumers.

Communications data is used to identify offenders and to demonstrate links between the suspects and victims, for example where an unlicensed bookmaker is conducting illegal gambling via the internet or over the phone.

Case study 1

Case/Investigation name: Operation Brahams

Communications data required: 7 subscriber checks, 2 reverse subscriber checks, 6 billing data and 6 traffic data**.**

Background/Reason for requesting data: A Commission investigation into unlicensed betting activities provided by a previously licensed operator who was

operating a telephone betting service through a network of local public houses. The investigation was launched following receipt of intelligence indicating the generating of considerable sums of money from the criminality.

Four communications data applications were submitted with 21 pieces of data being acquired. The use of targeted and focused applications enabled the investigators to identify the premises being used by the unlicensed operator, identify their associates, the phone numbers and identity of the pubs.

Ascertaining the volume of calls generated on specific days enabled a targeted intelligence led approach to focus maximum impact and disruption. Search warrants were obtained and executed recovering evidence including mobile phones associated to the communications data and used to facilitate the crime.

Outcome: This operation led to a successful prosecution with a guilty plea by the individual who received a non-custodial community sentence.

Would the outcome have been achieved without the data: The data identified essential elements of the offence, provided evidence of the volume of offending and linked the suspect to the premises within which the criminality occurred.

Case study 2:

Case/Investigation name: Operation Carp (ongoing)

Communications data required: Two of the applications are for phone data (5 subscriber details) and the remaining applications for internet related data: 3 IP subscriber details, 3 IP logon histories, 13 email subscriber details, 4 social media account subscriber details and 2 IP identifications from email headers.

Background/Reason for requesting data: A live complex Commission investigation relating to the provision of unlicensed betting activities marketed through social media targeting children and young persons. The illegal products offered are associated to social gaming and the investigation was commenced after receiving a complaint from a member of the public concerned that their child was gambling on a website.

Those involved operated with anonymity transacting through the internet and marketing through social media. Their activity was believed to be generating considerable financial reward and avoiding the payment of gambling duty.

The result of these applications allowed investigators to identify the individuals in control of the websites, the method of payment processing and the sending of confirmatory payment emails and the identity of those involved in marketing the products using social media. The IP addresses and IP identifications have helped show where and by whom the accounts were being managed, the date when accounts have been created, who created them and the location the accounts have been accessed from.

This enabled the collation of an evidential package supporting the obtaining of search warrants and the interviewing of those involved. Computers and phones used to facilitate the offences have been seized and the evidence is currently being considered by Commission Prosecutors.

Outcome: Ongoing investigation.

Would the outcome have been achieved without the data: The data obtained has been critical in focussing the investigation and assisting in obtaining evidence. This is an unusual and ground breaking investigation into an emerging area of gambling related criminality.

Gangmasters and Labour Abuse Authority

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Gangmasters and Labour Abuse Authority
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014 (as Gangmasters Licensing Authority)
• Applications: 20 • Notices & authorisations: 35

Requirement to be able to acquire communications data

The Gangmasters Licensing Authority, which will become the Gangmaster and Labour Abuse Authority (GLAA) later in 2016, was established under the Gangmasters (Licensing) Act 2004 following public concern at the lack of action to prevent the deaths of migrant cockle pickers in Morecambe Bay. It issues licenses only to approved gangmasters and investigates and prosecutes those without a license. Communications data can link unapproved gangmasters to the migrants they are exploiting, including cases of forced and compulsory labour and also money laundering.

On 13 May 2016, the Immigration Act received Royal Assent. This Act included new provisions to tackle labour market enforcement, and addressed the commitment in the Modern Slavery Act 2015 to review the role of the GLA in relation to the ability to tackle forced labour.

The new organisation will have a responsibility beyond the current licensed industries, and be able to investigate the forced labour offence, as well as other labour market offences that may facilitate forced labour. This expanded remit will increase the nature and scale of investigations carried out by the GLAA, and the necessity of the proportionate use of communications data to enhance the success of the investigations for which it will be responsible.

The GLAA will operate expanded Police and Criminal Evidence Act (1984) powers. It is therefore essential that all other supporting powers, such as the Regulation of Investigatory Powers Act 2000, Proceeds of Crime Act 2002, and new legislation, maintain and support the GLAA to be effective in its new role.

Case study 1:

Case/Investigation name: Operation 'A'

Communications data required: Subscriber and billing data

Background/Reason for requesting data: This case relates to the unlawful supply of workers into the GLA sector, contrary to Section 12(1) of the Gangmasters (Licensing) Act 2004. Intelligence suggested that a Lithuanian male was supplying workers recruited in Lithuania to food processing premises in the East of England.

Workers were charged large 'work finding' fees and provided with 'bonded' accommodation for which they were also over-charged (bonded accommodation is where individuals are tied to the accommodation through debt, threats or intimidation). Intelligence suggested there was a conspiracy between two male 'organisers' and also the possibility of involvement by a GLA licensed employment agency. Communications data was sought to provide evidence of the contact and frequency of contact between the relevant suspects. This information could not be obtained by other means without alerting the suspects to the criminal investigation.

Outcome: Communications data provided valuable evidence of communication and frequency of communication between the principal subjects. It also assisted the investigating officer to disprove the involvement of the GLA licensed agency in any criminality. The principle subject was convicted and sentenced to 7 years imprisonment. A parallel money laundering investigation was also conducted by Police Economic Crime Unit investigators.

Would the outcome have been achieved without the data: The call data analysis was intrinsic to developing the initial intelligence case which subsequently justified investigative tactics and specific lines of investigation and therefore helped lead to the conviction.

Case study 2:

Case/Investigation name: Operation 'B'

Communications data required: subscriber, billing and cell site data

Background/Reason for requesting data: This case relates to an investigation concerning the obtaining of a GLA licence by fraudulent means and the supply of workers into the GLA sector and beyond over a period of over 5 years. A Lithuanian male entered the UK in possession of the criminally obtained identity documentation of another EU (Dutch) citizen. This identity was then used over an extensive period to set up various companies, bank accounts and to purchase properties. A GLA licence was also obtained in the name of a labour provider business of which the fraudulent identity was a Director and Principal Authority. Following tentative GLA enquiries regarding his identity the subject allegedly left the UK leaving the business to be run by his spouse who claimed they were estranged. This was clearly a ruse intended to deflect the GLA from looking deeper into the business activities.

As it was clear there were prima facie significant criminal activity within and outside the GLA remit, the GLA approached the local Regional Asset Recovery Team to assist with a money laundering and fraud investigation to run in parallel with GLA offences – which they supported.

Outcome: Communications data was essential to this investigation as it provided evidence that the subject was in close association with his supposedly estranged spouse (the licensed gangmaster business) and also contacts responsible for the negotiation of labour provision contracts. Cell site data was used to focus other specialist activity on the principal subject. It also identified other subjects of interest to the investigation which otherwise may not have been revealed. The principal subjects were recently convicted at the Crown Court and given custodial sentences of 2½ and 3 years imprisonment respectively. A criminal business benefit sum in excess of £12 million has been identified and is subject of separate ongoing proceedings.

Would the outcome have been achieved without the data: Communications data proved invaluable to this investigation. It enabled focused lines of investigation to be pursued and ensured the proportionate and targeted use of specialist tactical options. Without the communications data, the above activity, which was essential to the investigation, may have proved unsuccessful or significantly extended the investigation in both time and cost to public funds.

Case study 3:

Case/Investigation name: Operation 'C'

Communications data required: subscriber and billing data

Background/Reason for requesting data: This case relates to the unlawful supply of workers into the GLA sector contrary to Section 12(1) of the Gangmasters (Licensing) Act 2004 and also offences of using the services of an unlicensed labour provider, contrary to section 13 of the Act. The GLA received intelligence suggesting that subjects were supplying workers from commercial premises in the Midlands area. Covert intelligence development work by GLA personnel identified two principle suspects who were subsequently arrested in possession of mobile telephones. Forensic analysis of the telephones identified a series of numbers and text messages which suggested the unlawful provision of labour.

Outcome: Communications data was sought in respect of the phone numbers the suspects had been contacting which provided evidence of contacts with a GLA licensed subject. When viewed in tandem with the text data found in the telephone handsets, this enabled GLA officers to interview the principle subjects gaining admissions of unlicensed supply and also using an unlicensed labour provider.

Would the outcome have been achieved without the data: Communications data enabled the GLA to validate the original intelligence and justification for covert and overt enforcement activity. It enabled the GLA to disrupt a network of criminals which prevented further exploitation of vulnerable workers**.**

Health and Safety Executive

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Health and Safety Executive
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder • (d) in the interests of public safety • (e) for the purpose of protecting public health
Communications data applications covering the period from January to December 2014
• Applications: 3 • Notices & authorisations: 11

Requirement to be able to acquire communications data

The Health and Safety Executive (HSE) enforces health and safety legislation. It investigates and prosecutes offences which involve the creation of serious risks to people, such as explosions from faulty domestic gas installations and major chemical incidents. It also takes action to prevent dangerous work from continuing or taking place. Communications data can be used to identify perpetrators, for example by placing them at the scene of a faulty installation.

Case study 1:

Communications data required: Telephone subscriber details.

Background/Reason for requesting data: An unregistered gas fitter carried out unsafe work on gas appliances and was traced by the HSE obtaining telephone subscriber details.

Outcome: The person was prosecuted by HSE and received a 6 month prison sentence.

Would the outcome have been achieved without the data: No. Without this information it wouldn't have been possible to bring a prosecution as the individual could not otherwise be traced.

Case study 2:

Communications data required: Telephone subscriber details.

Background/Reason for requesting data: An incident whereby a grandmother and her 8 and 15 year old grandchildren required significant medical treatment for carbon monoxide poisoning as a result of work undertaken on a gas boiler by an unregistered person. Telephone subscriber details of the person suspected of doing the dangerous work were obtained.

Outcome: Subscriber details were obtained which identified the name and address of the suspect thereby allowing the service of a Prohibition Notice to prohibit similar hazardous activities being carried out by that person**.**

Would the outcome have been achieved without the data: No. The opportunity to take action against this individual would have been missed and he may have only been identified after a further incident which could have led to fatal consequences.

Independent Police Complaints Commission

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Independent Police Complaints Commission • Office of the Police Ombudsman for Northern Ireland • Police Investigations and Review Commissioner
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder • (i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition— (i) to assist in identifying P, or (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition
Communications data applications covering the period from January to December 2014
Independent Police Complaints Commission • Applications: 13 • Notices & authorisations: 30 Office of the Police Ombudsman for Northern Ireland • Applications: 2 • Notices & authorisations: 2 Police Investigations and Review Commissioner • Figures not provided in Interception of Communications Commissioner report, 2015

Requirement to be able to acquire communications data

The Independent Police Complaints Commission (IPCC) undertakes independent investigations into the most serious cases of police criminality and misconduct, including deaths and serious injuries and other alleged human rights abuses. For example, if someone dies following contact with a law enforcement agency, the IPCC may acquire communications data to identify the deceased's movements prior to the incident and to identify potential witnesses.

Case Study 1:

Case/Investigation name: Misconduct in public office

Communications data required: Account information and call records.

Background/Reason for requesting data: An investigation into allegations that a serving police officer mishandled cases allocated to them for investigation. During the course of this investigation the mobile phone of the suspect was seized and forensically examined, revealing a large quantity a text messages between the suspect and another individual that appeared to be discussing collusion to pervert the course of justice.

Outcome: Account information was obtained which confirmed and evidenced the subscriber of the mobile phone in communication with the original suspect as a colleague within the same police unit. Call records confirmed the contact between the two mobile phones in line with the results of the forensic examination. The original suspect of the investigation was found guilty of five counts of misconduct in a public office.

Would the outcome have been achieved without the data: The evidence obtained from this application led to the second officer being referred to the CPS for consideration for charge for perverting the course of justice. Ultimately the CPS decided not to pursue these charges. The officer was however sacked following misconduct proceedings relating to the content of the text messages downloaded as a result of the initial forensic examination.

Case Study 2:

Case/Investigation name: Assault by a police officer

Communications data required: Call data records.

Background/Reason for requesting data: An investigation into allegations of assault by police officers following the stop of a motor vehicle containing 3 members of the public. Officers stated that the vehicle was stopped due to the driver using their mobile phone at the time and failing to stop for police. A communications data application was made to either corroborate or contradict the officers' accounts.

Outcome: Communications data was obtained which evidenced that the mobile phone was in use at the time of the incident, thus supporting the officers' account of what happened. This meant the additional consideration of perverting the course of justice was no longer appropriate, but one of the officers was found guilty of assaulting one of the passengers and given a 3 month custodial sentence, suspended for 1 year.

Would the outcome have been achieved without the data: No. The data obtained corroborated and added creditability to the account of the officer. This contributed to the decision for charges to be brought in relation to the assault alone and could not have been achieved by other means.

Information Commissioner's Office

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Information Commissioner
Statutory purposes under clause 58(7) available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• Applications: 28 • Notices & authorisations: 35

Requirement to be able to acquire communications data

The Information Commissioner is the independent supervisory authority responsible for enforcing the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. The Commissioner's Office (ICO) uses communications data where necessary to assist in identifying offenders attempting unlawfully to obtain, disclose, sell or offer to sell personal data in contravention of the above legislation.

Case Study 1:

Case/Investigation name: Suspected criminal breach of section 55 of the Data Protection Act 1998.

Communications data required: Subscriber information to include name, address, contact telephone numbers including full registration details, plus IP address connection history relating to the external email address to which the suspect sent 64 emails.

Background/Reason for requesting data: It was alleged that during a period of 2 months in 2015, an employee of the accident investigation department of a national hire car company had unlawfully sent in the region of 64 emails from their work email address to an external email address.

Each email contained details relating to accidents that had been reported to the hire car company and included data such as:

- Date and location of accident,
- Brief details of accident

- Time of accident
- Names of all drivers and passengers involved
- Mobile telephone numbers
- Registration numbers of all vehicles involved
- Details of who was at fault

This is a criminal offence contrary to section 55 of the Data Protection Act 1998. Personal information relating to approximately 550 data subjects was placed at risk. It is suspected that the data that was unlawfully obtained was then unlawfully passed on to commercial organisations. A large proportion of the data subjects were subsequently contacted by third-parties such as accident management companies, claim management companies and solicitors. The calls were unsolicited and related directly to the road traffic accidents that they were involved in. The purpose of the calls was to encourage the individual to pursue a claim for damages. It is this type of criminality that is helping to fuel the huge volume of unsolicited calls and texts suffered by UK citizens. Tackling unsolicited calls and texts is a priority for government and the ICO.

Outcome: In this case communications data was needed to identify who set up and owned the external email address that the personal information was sent to. Limited subscriber registration data was available but the date and time of registration, the IP address at the time of registration and the IP address connection history for the stated period were provided by the communications service provider. As a result, a further application requesting the subscriber details of the IP addresses that were provided was authorised and submitted to the relevant communication service providers in an attempt to identify the person who had created the external email address in question. No data was available regarding many of the IP addresses. However, two of the IP addresses resolved to the home address of the suspect. This investigation is ongoing and the evidence obtained from the IP address is pivotal to progress the investigation.

Would the outcome have been achieved without the data: No. Whilst the identity of the suspect was known, the communications data confirmed and corroborated that the suspect employee had unlawfully sent the emails to their own private account. This could not have been achieved by other means.

Case Study 2:

Case/Investigation name: Suspected criminal breach of section 55 of the Data Protection Act 1998.

Communications data required: Basic subscriber information to include name, address, contact telephone numbers, full registration details plus transaction information/IP connection history relating to the email account of the suspect.

Background/Reason for requesting data: A review of material held as part of an ongoing investigation identified emails between a known individual and an as yet unidentified person in 2003 which contained telephone account and billing information relating to an individual who was the subject of research/surveillance. It

is suspected that this personal data was obtained unlawfully contrary to section 55 of the Data Protection Act 1998.

Outcome: The communications service provider was able to provide subscriber data however, there was no IP data held. The resultant communications data has assisted in the identification of the second person and provided evidence supporting the offence contrary to Section 55 of the Data Protection Act 1998. This investigation is ongoing.

Would the outcome have been achieved without the data: No. This could not have been achieved by other means and the identity of the second person would not have been established without the communications data acquired.

Case Study 3:

Case/Investigation name: Suspected criminal breach of section 55 of the Data Protection Act 1998.

Communications data required: Basic subscriber information to include name, address, contact telephone numbers, full registration details plus transaction information/IP connection history relating to the email account of an unidentified person was requested in an attempt to identify the suspect.

Background/Reason for requesting data: A review of material held as part of this investigation identified an email from a known individual to an as yet unidentified person on 22/09/2003 in which they requested personal data from a number of data controllers in relation to mortgage details from two banks, national insurance or tax records, DVLA and driving license details belonging to a variety of data subjects.

Outcome: The communications service provider was able to provide registration data, however no IP data for the requested period was held. The resultant communications data has assisted in the identification of the second person and provided evidence supporting the offence contrary to section 55 of the Data Protection Act 1998. This investigation is ongoing.

Would the outcome have been achieved without the data: No, This could not have been achieved by other means and the identity of the second person would not have been established without the communications data acquired.

Local authorities

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Local authorities are covered by clause 69
Statutory purposes available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014 (this covers applications by all local authorities)
• Applications: 319 • Notices & authorisations: 2,110

Requirement to be able to acquire communications data

Local authorities are not included in Schedule 4 because they are covered by specific provisions elsewhere in the draft Bill. This is because they must go through a system of enhanced safeguards before being able to acquire communications data, including the requirement to make their requests for communications data through the Single Points of Contact at the National Anti-Fraud Network and magistrate approval. These safeguards were put in place to provide public reassurance following concern about isolated misuse of councils' surveillance powers several years ago.

Local authorities are responsible for investigating a range of serious offences, including under the Trade Marks Act 1994 and the Fraud Act 2006, such as scams targeting the elderly; rogue traders selling dangerous, illegal and counterfeit goods; environmental offences such as dumping hazardous waste illegally; and tenancy fraud.

Case study 1:

Case/Investigation name: Operation Magpie

Communications data required: Subscriber checks and call data

Background/Reason for requesting data: Operation Magpie concerned an investigation into an organised crime group who defrauded elderly and vulnerable people. The criminals exploited their victims to the extent that one person was evicted from their home. They also laundered cheques to the value of £700,000. Service use data for two mobile telephone numbers provided key information that enabled investigators to identify co-conspirators and a considerable number of victims.

Outcome: The ringleader of the gang received a prison sentence of 7 years with two co-conspirators receiving sentences of 5 years each. 16 other offenders were also convicted of money laundering offences serving prison sentences of up to 30 months.

Would the outcome have been achieved without the data: No. Without communications data it would have been extremely difficult to identify the scale of fraudulent activity and the number of individuals who were intimidated and defrauded.

Case study 2:

Case/Investigation name: Operation Troy

Communications data required: Subscriber checks

Background/Reason for requesting data: Operation Troy was a long running advanced fee fraud case. The fraud operated between 2007 and 2010, involved at least £7.5 million, affecting well over 16,000 consumers. Specifically, it involved two distinct frauds:

1. An escort/companion fraud in which consumers were offered guaranteed work as escorts and companions in return for a registration fee, however no work was subsequently provided.
2. A debt elimination fraud in which consumers paid an advanced fee to receive a debt elimination service but little or no service was ever provided.

The fraud was complex and well organised, operating from call centres in Spain. UK customers made contact with the call centres using free phone numbers that appeared to be UK based after viewing various escort websites offering work. During calls with escort agency staff, false promises would be made regarding the immediate availability of work and potential earnings available. Many consumers complained of similar experiences and provided similar accounts of last minute cancelled work appointments after they had paid their fees.

The escort websites and telephone numbers changed frequently to confuse consumers and make it difficult for enforcement bodies to track the source of the fraud. By obtaining communications data of the telephone numbers used for the fraud, the following links were established:

- The multiple telephone numbers were owned and operated by only two individuals. One of those individuals, who held the majority of the numbers, had been identified as being involved in operating multiple UK bank accounts used for money laundering aspects of the fraud and the creation of shell companies.
- All the UK free phone numbers were being redirected to Spanish based numbers that were linked to a small number of call centres operating from the Malaga area of Spain. These call centres were all owned by one man who was known to have a previous history of fraudulent trading.

- The link provided by this communications data provided evidence that what appeared outwardly to be over 12 different separate escort websites/agencies were in fact all one fraud perpetrated by one set of linked individuals.

Communications data was essential to the case, it was used to establish and evidence links between one of the main UK based defendants, and the multiple websites and telephone numbers set up to facilitate the fraud.

Outcome: In June 2012, European Arrests Warrants were applied for in respect of Antoni Muldoon, the man at the helm of the fraud, and two other members of the gang, Geraldine French and Bradley Rogers. All three were returned to the UK. Following extradition in September 2012, Muldoon pleaded guilty to conspiracy to defraud at Ipswich Crown Court.

Following Muldoon's plea, and after a series of trials at Ipswich Crown Court including a ten week trial involving five of the defendants that concluded in June 2013, seven further members of the gang were found guilty of offences including conspiracy to defraud and money laundering offences. The sentences handed down totalled 36 years overall, with Muldoon receiving 7.5 years for his role and Mark Bell of Ipswich, Muldoon's right hand man in the UK, receiving 6.5 years. Confiscation proceedings followed the sentencing and to date £315,000 has been awarded in confiscation and costs, which Suffolk Trading Standards has used to repay victims of the fraud.

Would the outcome have been achieved without the data: Utilising communications data significantly contributed to the success of the investigation. If communications data had not been available in this case, then the full scope of offending may not have been identified. Clear links to all other members of the conspiracy would have been harder to evidence, and further companies and associated bank accounts would have been harder to identify, and pursue under the Proceeds of Crime Act 2002. Significant criminal funds from the offending could therefore have remained undiscovered.

Case study 3:

Case/Investigation name: Suffolk County Council Trading Standards "clocked" car investigation.

Communications data required: Subscriber checks and call data

Background/Reason for requesting data: The victim replied to an online advert regarding a vehicle for sale. A meeting in person took place with the seller. After the victim had asked some questions about the vehicle, the suspect made a call on his mobile telephone to speak to someone in relation to the vehicle. This conversation was not in English; therefore the victim was unaware of the nature of the call. The vehicle was purchased for £7,500 and was later found to have been "clocked" – meaning that it appeared to have been driven a shorter distance than it actually had. The suspect was interviewed in connection with the offence. In his defence he stated that he had made a number of phone calls to a specific individual, and it was

this individual who owned the vehicle. The suspect was only a 'middle man' in the transaction. Around the time of the sale, he said he made a number of calls to a named person. A record of outgoing calls from the suspect's telephone made during the meeting with the victim was obtained. The suspect claimed that he was speaking to his girlfriend at the time of the call. Subscriber checks on the telephone numbers dialled during this time were then acquired. The results of the subscriber checks refuted this and undermined his defence.

Outcome: The offender was summonsed for offences of fraud by false representation and Proceeds of Crime Act 2002 money laundering. He was found guilty at Ipswich Crown Court and received a 3 month custodial sentence (suspended for 18 months) and was ordered to complete 120 hours of unpaid work. A financial investigation revealed large sums of money in his bank accounts, he was also ordered to make proceeds of crime payment of £100,157 and a Jaguar vehicle was seized with a value of £22,500. Part of the judge's comments in sentencing were that he was a "deeply dishonest man".

Would the outcome have been achieved without the data: The results were used to undermine a defence given in the interview. The communications data evidence was shared in court and used by the legal team to suggest that the suspect was dishonest. This was on the basis that he said one thing but the facts showed something else. This contributed to the defendant being found guilty, in conjunction with the other facts.

Case study 4:

Case/Investigation name: Illicit Alcohol

Communications data required: Subscriber checks

Background/Reason for requesting data: This investigation concerned the illegal supply of illicit alcohol from a local off licence, involving 24 bottles of suspected counterfeit vodka which was on sale and available to the public. The products were immediately seized by trading standards officers and tested for alcoholic strength and compositional analysis. The results identified the vodka contained a significant amount of methanol (22 times over the legal limit). Methanol is a substance which is often used in fake vodka and can cause permanent blindness. The retailer claimed the vodka was purchased from a man he regularly met at the cash and carry and also around the area in which he lived. The man provided the retailer with telephone numbers if he wanted to purchase anymore.

Outcome: The retailer was prosecuted under the Food Safety Act and pleaded guilty and the communications data allowed a subsequent investigation into the supplier of the counterfeit vodka.

Would the outcome have been achieved without the data: Without communications data it would have been very difficult to identify the supplier and to therefore protect others.

Ministry of Justice

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Ministry of Justice • Department of Justice in Northern Ireland
Statutory purposes available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder • (d) in the interests of public safety# Department of Justice in Northern Ireland also are also able to use the following statutory purpose: • (i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition— (i) to assist in identifying P, or (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition
Communications data applications covering the period from January to December 2014
Ministry of Justice • Applications: 55 • Notices & authorisations: 84 Department of Justice in Northern Ireland • Applications: 0 • Notices & authorisations: 0

Requirement to be able to acquire communications data

The National Offender Management Service (NOMS) of the Ministry of Justice acquires communications data in order to investigate allegations regarding crime committed under the Prison Act 1952. Often investigations will be linked to corruption allegations against prison staff or official visitors to the prison and communications data is critical to establish a connection between a member of staff and a prisoner.

Some of these investigations concern the supply of illegal drugs and illicit telephones in prisons. The illicit use of mobile phones across the prison estate is one of the most significant threats currently facing NOMS and the increased use of drugs, including psychoactive substances, is associated with increasing violence in prisons. Illicit mobile phone use undermines good order and control in prisons and perpetuates

ongoing criminality both inside and outside of custody, including serious and organised crime and extremism. On another level, videoing and uploading to the internet acts of violence in prisons is a growing concern.

In March 2015, the Serious Crime Act received Royal Assent. Section 80 of the Act created the legal basis for Telecommunication Restriction Orders. These court orders will allow NOMS to compel Mobile Network Operators (MNOs) to disconnect illicit mobile phones and SIM cards being used in a prison. NOMS is working on the secondary legislation necessary to enact the orders, as well as working with MNOs to finalise the process. NOMS has committed to utilising communications data as part of the analysis process to prove that mobiles initially identified as being in a prison are actually present in the establishment.

Without the capability to acquire communications data, an important tactic for the investigation of crime in prisons would be unavailable to NOMS. Prisons would be less secure and threats to security and/or the rehabilitation of prisoners undermined.

Case study 1:

Case/Investigation name: HMP Birmingham

Communications data required: Subscriber and incoming and outgoing call data

Background/Reason for requesting data: Investigation into misconduct in a public office, more specifically an inappropriate relationship between a member of staff and several prisoners. Intelligence suggested that the subject was supplying drugs and mobile phones into the establishment, conducting inappropriate emotional and sexual relationships with prisoners, and was engaged in the unauthorised disclosure of information to prisoners. The aim of the operation was to analyse communications data against information already held by the prison to identify links to prisoners and any other associates involved in suspected criminal activity.

Outcome: The subject was convicted of misconduct in a public office (x5) and possession with intent to supply a controlled drug. The subject was sentenced to 2 years and 8 months in custody.

Would the outcome have been achieved without the data: No. Communications data was a key tactic in the investigation and used to link the subject to prisoners and the evidence of inappropriate relationships. The subscriber check yielded a positive result, matching the relevant phone number to the subject. Call data was also analysed alongside other sources of intelligence. As an example, incoming call records on the target number were cross checked against outgoing calls made by prisoners on the prison telephone system.

Case study 2:

Case/Investigation name: Hypothetical

Communications data required: Location information

Background/Reason for requesting data: Communications data may need to be sought to determine whether phones are being used in prison. For example, where criminals are using phones to harass people through social media, communications data could determine the devices being used in the vicinity of prisons and the times they are used.

Outcome: Acquiring communications data may be the only way to determine that a phone is being used in a prison at the same time as the victim is receiving abuse through social media.

Would the outcome have been achieved without the data: Where mobile phones are not found in searches, communications data is often the only way to demonstrate that they are being used by prisoners and in prisons.

National Health Service Business Service Authority

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• National Health Service Business Service Authority • Common Services for the Scottish Health Service • Northern Ireland Health and Social Care Regional Business Services Organisation
Statutory purposes available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
National Health Service Business Service Authority • Applications: 4 • Notices & authorisations: 10 Common Services for the Scottish Health Service • Applications: 0 • Notices & authorisations: 0 Northern Ireland Health and Social Care Regional Business Services Organisation • Applications: 0 • Notices & authorisations: 0

Requirement to be able to acquire communications data

NHS Protect is the body charged with tackling crime within the NHS, including having responsibility for leading investigations into serious, organised and/or complex financial irregularities and losses which give rise to suspicions of fraud, bribery or corruption. Communications data is used to demonstration links between conspirators, for example those involved in the production of fraudulent invoices for substantial sums of money.

The following cases demonstrate the public benefit of the body charged with tackling crime within the NHS being able to acquire communications data. A failure to retain access to communications data would place NHS funds at a significantly higher level of threat.

Case study 1:

Case/Investigation name: Operation Lamont

Communications data required: Telephone subscriber details

Background/Reason for requesting data: This case involved a £200,000 insider-enabled invoice fraud. The acquisition of communications data in this investigation proved essential to demonstrating the guilt of the defendants.

Outcome: Charges of conspiracy against 5 offenders were subsequently brought, who all pleaded guilty to the offence. There was also a charge of money laundering for a sixth defendant who also pleaded guilty. Without the communications data evidence there would have been a significant risk that the defendants would have been in a position to contest the charges. This evidence proved knowledge of the fraud and through the communications data evidence it was established that the defendants were linked to the relevant telephone numbers. Equally, this evidence established the links between phones and conversations and between the conspirators.

The Interception of Communications Commissioner has made specific reference to the value of communications data to the successful conclusion of this case:

"Communications data was crucial in progressing a number of serious fraud investigations. One such example is Operation Lamont, an investigation into an invoice and diversion of payroll fraud directed against an NHS Trust. A financial analyst employed by the Trust was arrested and a search of his home led to the forensic examination of two Blackberry devices seized in evidence. Text messages stored in the devices were incriminating and indicated the roles of a number of co-conspirators. Applications for communications data under Section 21(4)(c) identified the co-conspirators. The 6 defendants pleaded guilty at Southwark Crown Court. The Trust employee received a 21 month imprisonment term and the other defendants received suspended sentences and community support orders dependent on their degree of involvement."

Would the outcome have been achieved without the data? Without access to communications data it would not have been possible to demonstrate the extent of the connections between the conspirators to support criminal prosecution

Case study 2:

Case/Investigation name: Operation Solent

Communications data required: Telephone subscriber and billing

Background/Reason for requesting data: This investigation involves a conspiracy to defraud the NHS (via diversion of a Trust's payments to its suppliers) totalling circa £640,000.

Outcome: Eight subjects were successfully convicted with a range of custodial sentences. The use of communications data within this investigation was instrumental in demonstrating the range and depth of conspiracy between subjects, using registration and billing data across 19 mobile devices to evidence the level and timing of communication taking place prior to diversion and transference of moneys across a range of bank accounts. The communications data retrieved demonstrated that contact was made with recipients of payments on the days those payments went into their accounts as well as contact being made with suspected money launderers on the days when monies were transferred into their accounts.

Would the outcome have been achieved without the data? Without this data being made available it is unlikely that sufficient evidence would have been available to secure all charges relating to conspiracy and money laundering.

Case study 3:

Case/Investigation name: Operation Evergreen

Communications data required: IP subscriber / telephone subscriber / telephone billing / SIM details / email subscriber

Background/Reason for requesting data: This investigation involved fraud by abuse of position and money laundering by two subjects, one of which was the Continuing Care Manager at the NHS Trust. False invoices for over £117,000 for the continuing care of a number of fictitious patients were created and paid out of the Continuing Care budget.

Outcome: This resulted in the successful conviction of two subjects both of whom received substantial custodial sentences. Communications data was key in linking the Continuing Care Manager at the trust with the fraud and the other subject. The IP login history associated with the email account allowed the investigator to demonstrate that when the subject was out of the country the fraud continued to be orchestrated from Nigeria and when the subject returned to the UK the email account was accessed from a connection that was traced back to the subject's home broadband connection.

Would the outcome have been achieved without the data? In the course of this investigation ten applications for communications data were made which provided substantial contribution to the evidence in this case. The IP details were particularly pertinent making an irrefutable link between the fraud and the subject. Without the data obtained as a result of these applications it is considered unlikely that sufficient evidence would have been available to be confident of a guilty verdict.

Office of Communications

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Office of Communications
Statutory purposes available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• Applications: 21 • Notices & authorisations: 58

Requirement to be able to acquire communications data

The Office of Communications (Ofcom) is the UK communications regulator. One of its duties is to protect and manage the radio spectrum relied upon by a vast range of devices and services including our mobile phones, broadcast TV and radio, as well as communications networks for the emergency services.

The radio spectrum is a finite and valuable resource that requires protection from interference in order to ensure optimal use is made of it. This includes taking steps to stop interference from those who are not authorised to use the spectrum, like unlicensed radio broadcast stations, and removing non-compliant radio and electrical apparatus from the market. Illegal broadcast stations regularly cause interference to the frequencies used by aircraft for communications and navigation, and any interference to the spectrum has the potential to cause dangerous disruption to important spectrum users like the emergency services.

Illegal broadcasting, otherwise known as pirate radio, is the operation of an unlicensed and unregulated radio station. There are about a hundred illegal stations in the UK with around three quarters based in London. Their apparatus is often installed on high rise local authority owned residential buildings. They use sophisticated techniques to avoid detection, streaming content and controlling stations via the internet.

It is a criminal offence to be involved with an illegal broadcast station. Likewise to place non-compliant apparatus on the market. Ofcom uses communications data to obtain evidence as a part of the criminal investigation process to identify and convict offenders. Enforcement is a key tool in detecting and preventing illegal broadcasters and is seen as an effective deterrent. Ofcom was responsible for 16 convictions in the last year.

Case study 1: Unknown FM

Case/Investigation name: Unknown FM is an illegal broadcast station that operates in London. The station uses high power radio transmitters installed illegally on rooftops of high rise local authority owned properties. Those involved in the station sought to isolate themselves from the transmitter using the internet to stream content and control the apparatus.

Communications data required: IP login information and account details relating to email addresses.

Background/Reason for requesting data: Ofcom needed to identify those running the station. During a raid on the station's studio, Ofcom seized documents containing IP and email addresses. However, it had no means of identifying the relevant people associated with these addresses without obtaining communications data.

Outcome: The data Ofcom obtained from the relevant communications service provider enabled Ofcom to identify a suspect and enforcement action was taken against him.

Would the outcome have been achieved without the data: No. Those running the station had taken steps to run it remotely, using aliases, to avoid detection. Ofcom had no means of identifying them other than the IP addresses and the communications data was used to connect those addresses with the individuals.

Case study 2:

Case/Investigation name: Fresh Soundz an illegal broadcast radio station.

Communications data required: Subscriber details of a mobile phone number and device details linked to the mobile number used by the station.

Background/Reason for requesting data: The broadcast station operated by using high power radio transmitters installed illegally. Those involved in the station used the internet to stream content and control the apparatus involved in broadcasting the station. Ofcom raided the station's studio and seized equipment including a computer attached to the transmitter. It retrieved a mobile phone number from a log file on the computer, which investigations showed had been used to remotely access the computer.

Outcome: Ofcom obtained communications data that disclosed the identity of the subscriber to the relevant telephone number and data that showed the device used to control the transmitter. Enforcement action was taken against the suspect who was subsequently convicted at Crown Court.

Would the outcome have been achieved without the data: It is unlikely that the suspect would have been identified without communications data because this was the only evidential link between an identifiable individual and the illegal broadcast.

Case study 3:

Case/Investigation Name: Various West Midland illegal broadcast stations.

Communications data required: Registration information of an IP address, account information for two telephone numbers and registration details of an email address.

Background/Reason for requesting data: This investigation was to target seven illegal broadcast stations and to identify those involved in facilitating their operation by providing the technical internet support. The stations were all operating in the Birmingham area using the internet to stream content and remotely operate their transmitters via computers. Ofcom seized computers when raiding some of the studios used by the stations, and retrieved the relevant IP and email addresses, and telephone numbers, from them.

Outcome: The communications data obtained showed that the IP and email addresses and the telephone numbers used in connection with the running of the station were registered to one individual. This helped to prove he had facilitated the operation and day to day running of seven stations.

Would the outcome have been achieved without the data: The communications data was pivotal. It enabled Ofcom to establish the identity of the relevant individual and to use that information to help identify all the premises used as studios, obtain search warrants and subsequently to obtain a conviction of the individual.

Serious Fraud Office

Which entries in Schedule 4 of the Investigatory Powers Bill this includes
• Serious Fraud Office
Statutory purposes available to these authorities
• (b) for the purpose of preventing or detecting crime or of preventing disorder
Communications data applications covering the period from January to December 2014
• Applications: 32 • Notices & authorisations: 50

Requirement to be able to acquire communications data

The Serious Fraud Office (SFO) has a key role in protecting the UK from the huge losses associated with serious organised economic crime, including large scale bribery and corruption and targeted attempts to manipulate the London financial markets.

Current SFO cases, for example, relate to the rigging of international financial markets, as well as corruption in international defence, aerospace, and pharmaceutical contracting. The SFO also plays a key role in assisting international partners in fighting complex fraud, which includes the receipt of mutual legal assistance requests, requiring communications data in respect of such cases. This type of law enforcement work therefore goes to the heart of the national economy, and has major international significance, not least because it provides a significant deterrent.

As well as prosecuting suspected offences perpetrated by individuals and corporations, the SFO also investigates real-time economic crimes. The latter, in particular, can require fast time identification and location of individuals engaged in serious criminal conduct; from recent phone usage to internet access information. Speedy access to communications data is vital to the execution of executive action, such as arrest and search, and the securing of primary evidence to prosecute suspects.

Communications data sought by the Serious Fraud Office includes:

- Cell site and information showing the location of a device (both historic and live trace), IP history and incoming calls;
- Itemised telephone call records, forwarding and redirection;

- Subscriber information such as subscriber checks, comprehensive account information, IP address at registration and equipment information.

If the SFO were unable to acquire communications data it would have a significant impact on the core business of the SFO and its role to help safeguard the UK's reputation as a safe place to do business, ensure top level fraudsters and corruptors cannot operate with impunity, and help create a level playing field for businesses. Without recourse to the full range of communications data currently available to the SFO, capability to properly investigate and prosecute top tier economic crime would be substantially diminished.

Case Study 1:

Communications data required: Subscriber and call data

Background/reason for requesting data: The fraudsters 'sold' but failed to supply thousands of tickets for events including international sporting events and music festivals. Their companies collapsed leaving more than 10,000 people without tickets and causing substantial losses. They tried to blame this on their supplier.

The communications data applications related to mobile telephone numbers that were on invoices from the supposed supplier. The data showed that the telephones were unregistered pre-pay telephones with a very low number of short duration calls over a long period. It was presented in Court to demonstrate that the 'ticket suppling company' was a sham, and to discredit the defendants' account that the supplier had stolen the money.

Outcome: One defendant pleaded guilty and two were convicted after trial. Sentences of eight years, seven years and two years eight months were handed down. Two directors were disqualified from acting as a company director for 10 years and 15 years and further sentences were handed down for failing to pay confiscation orders.
Compensation was obtained for all customers who had contacted the SFO or Metropolitan Police and who could not claim back their losses on the credit cards. Serious Crime Prevention Orders will take effect when the defendants are released from custody.

Would the outcome have been achieved without the data: The data played a central role in undermining the defence case.

Case Study 2:

Communications data required: Subscriber checks, call/message data, historical cell site information and cell site data.

Reason for requesting data: This investigation involves a serious offence of paying a substantial bribe of approximately $1m to secure a multi-million dollar business contract contrary to the Bribery Act 2010.

Outcome: This case is not yet concluded, but the communications data has been of considerable benefit to the investigation, in demonstrating that a particular mobile telephone was being used by the principal suspect. A subscriber check linked this number to a co-suspect and cell site data led to the identification of the address the principal occupied. The communications data also later provided evidence of the suspect's subsequent efforts to evade arrest at this address.

Would the outcome have been achieved without the data: No. Evidence of the suspect's whereabouts and attempts to evade arrest would not have been obtained without the requested data – this aspect forms part of the prosecution's case.

Case Study 3:

Communications data required: Details of all handset identifiers associated with a telephone number and telephone data since the account was opened.

Reason for requesting data: This is an investigation into bribery and corruption involving significant bribes to secure multi-million dollar contracts. Upon arrest the suspect produced a mobile phone believed to be of vital importance to the investigation. When forensically examined the handset contained considerably less information than expected. The suspect then failed to comply with a Notice compelling him to produce any further mobile telephones in his possession. Investigators believed the individual had deliberately not produced the actual handsets subject to the Notice in order to conceal incriminating evidence. The purpose of requesting communications data was to prove the offence of concealing evidence contrary to the Criminal Justice Act, for which a conviction on indictment carries a maximum sentence of 7 years imprisonment.

Outcome: The communications data demonstrated the suspect had swapped a SIM card into a different handset prior to surrendering it upon arrest. This was corroborated via itemised billing data which showed there was a missing handset and that it had been used pursuant to corrupt activity. The suspect was subsequently charged with concealing evidence on the strength of the communications data.

Would the outcome have been achieved without the data: No. It would not have been possible to demonstrate the factual swapping of the handset and implied guilty knowledge of the suspect without recourse to communications data.

Case study 4: Hypothetical example

Communications data required: Internet connection records.

Reason for requesting data: To help combat an ongoing international money laundering operation by identifying bank accounts accessed by individuals involved, and their travel details.

In this hypothetical example, an Organised Crime Group (OCG) could be involved in laundering multi-million pound proceeds from the corrupt sale of mineral extraction

rights by a regime in Africa via the UK. Analysis of suspected members of the OCG's internet connection records may demonstrate, for example, the travel agent that the suspects use. The SFO would then be able to obtain from the travel agent details of the suspects' planned and previous travel to and from the UK. Furthermore, the internet connection records may also be able to demonstrate the online banking services that the suspects were using, potentially helping the SFO to determine how the suspects launder the money.

Outcome: Without internet connection records there would be a significant part of the intelligence picture missing, making it far more difficult for the SFO to determine the travel arrangements of the suspects and how they are laundering the proceeds of their criminal activities.

Would the outcome have been achieved without the data: Although hypothetical, the example is nonetheless realistic and internet connection records could be essential for such investigations.