EXPLANATORY MEMORANDUM TO

THE REGULATION OF INVESTIGATORY POWERS (COMMUNICATIONS DATA) ORDER 2010

2010 No. 480

1. This explanatory memorandum has been prepared by the Home Department and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 The purpose of this Order is to:

a) consolidate three previous Orders relating to the acquisition of communications data by public authorities under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('RIPA'); and to

b) reflect the outcome of a public consultation which took place between April and July 2009.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

4. Legislative Context

4.1 This Order consolidates three previous Orders (revoked by article 9 of this Order) made under the same powers. The Order requires approval by resolution of each House of Parliament and will come into force on 6th April 2010.

4.2 Chapter II of Part I of RIPA ("Acquisition and Disclosure of Communications Data") provides a statutory framework governing the acquisition of communications data by "relevant public authorities", and its disclosure by postal or telecommunications operators, consistent with the Human Rights Act 1998.

4.3 Column (1) of the Schedules to the Order lists the "relevant public authorities" for these purposes. Column (1) of Schedule 1 contains the public authorities already listed in RIPA. Article 3(3) and column (1) of Schedule 2 of the Order specify additional public authorities as "relevant public authorities". The only substantive changes made by the Order to the list of relevant public authorities are as follows. Schedule 2 contains three additional relevant public authorities: the Child Maintenance and Enforcement Commission, the Northern Ireland Office and the Department of the Environment in Northern Ireland. The Northern Ireland Office and the Department of the Environment in Northern Ireland may already authorise directed surveillance and covert human intelligence sources under Part II of RIPA (in the case of the Department of Environment under Statutory Rule 2002 No.292 Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order (Northern Ireland) 2002).

4.4 Designated persons with a relevant public authority may grant authorisations or give notices to obtain communications data. Columns (2) and (3) of Schedules 1 and 2 to the Order identify the designated individuals holding offices, ranks and positions with the relevant public authorities who may acquire communications data. All more senior individuals to those listed in column (2) of Schedule 1 or column (2) of Schedule 2 may acquire communications data in the same circumstances and subject to the same restrictions to those to whom they are senior.

4.5 Article 5 and column (4) of the Schedules to the Order impose restrictions on the "purposes" for which communications data may be acquired by the public authorities identified in column (1). The Order includes additional purposes for the Serious Organised Crime Agency ("in an emergency to prevent death or injury") and the Independent Police Complaints Commission and Ministry of Justice ("identifying a person"). The Order also removes purposes for the Food Standards Agency ("public safety"), Health and Safety Executive ("in an emergency to prevent death or injury") and the Ports Police ("in the interests of national security").

4.6 Other minor amendments made by the Order are as follows. The Order removes the restriction in article 10 of S.I. 2003/3172 which currently prevents individuals in Her Majesty's Revenue and Customs ("HMRC"), in connection with functions relating to former Inland Revenue matters, from acquiring traffic data that does not relate to a postal service. The Order also amends article 7 to enable the Department of Transport Accident Investigation Branches to acquire service use and traffic data.

5. Territorial Extent and Application

5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

6.1 David Hanson, Minister of State for the Home Department has made the following statement regarding Human Rights:

"In my view the provisions of the Regulation of Investigatory Powers (Communications Data) Order 2010 are compatible with the Convention rights."

7. Policy background

7.1 Communications data is information held by communication service providers relating to the communications made by the users of their services. Acquisition of communications data is a vital investigative tool that can reveal associations and events by time and location and it has proven benefits in terms of helping secure successful convictions. Communications data can confirm who communicated with whom, when and, for mobile communications, where (but not what was said or written). This includes itemised call records, routing information and subscriber details.

7.2 Parliament has already debated and approved most of the provisions in this Order, providing that listed public authorities may lawfully authorise the acquisition of communications data for a specific purpose where it is necessary and proportionate to

do so in line with Convention rights. Following the debate in June 2006 in relation to S.I 2006/1878 the Minister of State, Tony McNulty, gave a commitment to consolidate the RIPA Orders. By consolidating and updating the previous Orders the Department aims to provide clarity on the public authorities able to authorise the acquisition of communications data. The consolidated Order reflects the results of a public consultation outlined at 8.1 below and provides in one place a list of those public authorities which have a legitimate requirement within the regulation provided by RIPA to interfere with an individual's right to privacy.

7.3 The relevant public authorities, augmented by the authorities identified in 4.3 above, who may acquire communications data under RIPA are as follows:

Ambulance Services

Ambulance Services across the UK use communications data to locate callers in an emergency where the caller is unable to give their position or to contact relatives or next of kin to give relevant details of patients, thus preventing death and serious injury. Communications data also provides details to police investigations on assaults on staff and inappropriate calls.

Armed Service Police

The Royal Navy Police, Royal Air Force Police and Royal Military Police provide support for the Armed Services operating in the UK and overseas as well as policing the Services themselves. They use communications data to prevent and detect crime against or on Armed Service property, establishments and personnel (such as countering hostile surveillance) and any crime committed by Service officers.

Charity Commission

The Charity Commission is the statutory regulator of charities in England and Wales. It investigates charity misconduct or mismanagement such as fraud, money laundering, links to terrorist organisations, sham charities set up for improper or illegal purposes or for private advantage or the abuse of vulnerable beneficiaries. This allows the public to be confident that the money given to charities actually does go to the good causes represented.

Child Maintenance and Enforcement Commission

The Child Maintenance and Enforcement Commission would use service use and subscriber data in criminal investigations to locate and prosecute non-resident parents who disappear after failing to co-operate with requests for information by the Commission or to prosecute where they knowingly provide false information in connection with their financial situation. There are some 5,000 non-resident parents, in relation to whom other investigatory techniques cannot be deployed successfully, with the result that communications data is the only viable technique. The Interception of Communications Commissioner's Office has agreed that the Child Maintenance and Enforcement Commission's need is proportionate. The ability to obtain communications data and take action in these cases would translate to an estimated £40 extra per week on average being made available for children receiving no or minimal support from absent parents.

Civil Nuclear Constabulary

The Civil Nuclear Constabulary uses communications data to protect designated civil nuclear sites by preventing or responding effectively to security breaches in segregated nuclear areas. It also provides secure, armed escorts for the storage and movement of civil nuclear materials

in the UK and abroad, and ensures an effective armed response in the event of terrorist targeting.

Criminal Cases Review Commission / Scottish CCRC

The Criminal Appeal Act 1995 and the Criminal Procedure (Scotland) Act 1995 provide for the Criminal Cases Review Commission and the Scottish Criminal Cases Review Commission respectively to investigate alleged miscarriages of justice. They affirm the safety of convictions, thus reinforcing everyone's right to a fair trial under ECHR and promoting confidence in the effectiveness of the criminal justice system. Communications data enables the Commissions to determine salient facts to support or undermine assertions made by people claiming wrongful conviction. This includes verifying an applicant's location at the time of the crime or proving/disproving that a call was made at the material time.

Department of Agriculture and Rural Development

The Department of Agriculture and Rural Development has statutory enforcement responsibilities for a wide range of animal health and welfare issues in Northern Ireland, including traceability and disease control offences committed in abuse of the border with the Republic of Ireland. It uses RIPA in such areas as illegal cattle movement, the illegal importation of meat products and veterinary medicines, and the investigation of cases of suspected internal and external fraud, where necessary tracing subsidy and compensation fraud back to Department staff.

Department for Business, Innovation and Skills

The competition regulator is able to use RIPA to prevent or detect crime or disorder relating to a range of anti-competitive business offences. This includes investigating and prosecuting offences under the Companies Act, Insolvency Act, Fraud Act and Theft Acts such as insolvency fraud, unscrupulous trading practices and breaches in employment legislation. Effective regulation of commercial practices boosts UK productivity, protects the consumer, expands choice and provides better value.

Department of Enterprise, Trade and Investment

The Department of Enterprise, Trade and Investment for Northern Ireland uses communications data to undertake the same functions as the Heath & Safety Executive and local authority trading standards in England, Wales and Scotland. This includes safeguarding the interests of consumers and ensuring health, safety and welfare at work.

Department for Environment, Food and Rural Affairs

DEFRA Investigation Services enforce legislation relating to animal welfare (eg foot and mouth disease) and investigate crime and compensation and subsidy fraud covering a wide range of subjects (such as cattle identification, tree felling, veterinary medicines, use of pesticides and plant health). They use communications data mainly to trace the sellers of illegal veterinary medicines and investigate offences contrary to the Dairy Produce Quota Regulations (the supply of milk outside the quota system).

DEFRA's Marine and Fisheries Agency enforces legislation governing fishing at sea, including catch-quotas, fish and mesh sizes, foreign fishing rights and the fish's journey to first sale. The benefit of offending is worth millions of pounds to individuals and disrupts the fish economy for the majority.

DEFRA's Centre for Environment, Fisheries and Aquaculture Science enforces regulations to prevent the spread of serious disease in England and Wales freshwater fish and shellfish stocks. This applies both to stocks kept for farming and sport. Communications data tackle the illegal importation of fish by determining addresses of offenders and gathering evidence of illegal importation. Circumventing these controls would have potentially serious effect in terms of the spread of any fatal disease introduced to the country.

Department of the Environment

The Department of the Environment in Northern Ireland would use service use and subscriber data to identify and prosecute landowners complicit in large-scale industrial dumping of hazardous waste amounting to thousands of tonnes each year. The authority faces potential EC infraction proceedings if it cannot take effective action against environmental pollution. The problem is compounded by close proximity to the Republic of Ireland and higher disposal rates south of the border, leading to the illegal disposal of waste from the Republic north of the border. The Home Office intends to limit the authority's access to the purposes of preventing or detecting crime or preventing disorder, and protecting public health. This is broadly in line with equivalent departments in the rest of the United Kingdom.

Department of Health – Medicines & Healthcare Products Regulatory Agency

The MHRA is the statutory enforcement agency responsible for ensuring that medicines and medical devices are tested, work and are acceptably safe. It investigates and prosecutes breaches in the control of licensed medicines, including unlicensed or counterfeit medicines supplied on the internet, stored in warehouses or sold in retailers. It also investigates and prosecutes suppliers of counterfeit medical devices. Unfit supplies that are known to have reached consumers in the UK include condoms and dental material for use in fillings. Incidents of counterfeits stopped before reaching consumers include glucose test strips for use in conjunction with insulin, and corrective contact lenses. If not prevented or taken out of circulation, unlicensed, unlawful or counterfeit medicines and medical devices can lead directly to reduced quality or even loss of life.

Department for Transport – Accident Investigation Branches

The Air Accident Investigation Branch, the Marine Accident Investigation Branch and the Rail Accident Investigation Branch are all administratively part of the Department for Transport but function independently in the conduct of their investigations. Their primary purpose is to determine cause of accident with a view to preserving life, improving safety and preventing future occurrences – not to apportion blame or liability. An integral part of the investigations is ascertaining whether the use of telecommunications by drivers, pilots or others played any part in the incident (which may include loss of life).

Department for Transport – Maritime and Coastguard Agency

The Maritime and Coastguard Agency is an on-call emergency organisation responsible for the initiation and co-ordination of all search and rescue operations within the waters for which the UK has responsibility. This includes using communications data to locate and respond to missing vessels at sea, persons either in distress at sea, or to persons at risk of injury or death on the cliffs or shoreline of the UK (where HM Coastguard has a statutory responsibility to co-ordinate a response to save life or prevent injury).

The agency is also the UK regulatory authority for ships and shipping in respect of safety and pollution matters. Communications data are used to investigate and prosecute breaches of the Maritime Shipping Act (relating to the safe construction and operation of both cargo and

passenger craft) and anti-pollution legislation (including tracing responsibility for and taking action against those responsible for oil or chemical spills).

Environment Agency / Scottish Environment Protection Agency

The agencies are the leading public bodies for environmental regulation and advice in England, Wales and Scotland. They are responsible for combating pollution and protecting and improving the environment. In addition to helping business and industry understand their environmental responsibilities, they enforce against illegal activity, including tackling large-scale illegal waste dumping, the running of unregulated landfill sites and unauthorised discharges of polluting substances to the environment. Fly-tipping on agricultural land alone costs society £60 million a year, as well as damaging the local environment and potentially harming those who live there. The agencies also tackle organised criminals perpetrating large-scale, geographically dispersed environmental crimes, including international illegal exports of waste.

Financial Services Authority

The UK's financial regulator has statutory responsibilities for investigating and prosecuting particular criminal offences to maintain market confidence. Communications data are used mainly in the investigation and prosecution of insider dealing under the Criminal Justice Act 1993. Other investigations in which covert techniques have been used include unauthorised collective investment schemes under the Financial Services and Markets Act 2000. The FSA is increasingly involved in detecting criminal activity on the internet. Unless these kinds of professional financial collaboration are addressed effectively they would operate against the consumer's interests and could damage the integrity of UK financial markets.

Fire and Rescue Services

Fire and rescue services across the UK attend fire incidents at domestic and commercial premises (including oil and gas terminals, power stations, airports, docks etc) and serious road accidents. They are also responsible for enforcing regulations concerning fire safety. This work enables them to save lives and protect property and the environment. Communications data are used in connection with taking enforcement action in support of explosive and petroleum regulations or deliberate fire setting to help piece together the sequence of events, progressing accident investigations (for instance where fire fighters are injured at the scene of a fire) and detecting inappropriate calls.

Food Standards Agency

The Food Standards Agency was created under the Food Standards Act 1999 to protect the public by enforcing statutory food safety standards. It inspects meat at slaughterhouses and processing plants to ensure that the standards required by the law for hygienic production and animal welfare at slaughter are maintained. Its enforcement team considers the use of communications data to prevent unfit meat from entering the market for human consumption. If it does not have covert techniques to use when it needs to, there could be serious public health consequences and the consequences for some consumers could be fatal.

Gambling Commission

The Commission was set up under the Gambling Act 2005 to regulate the gambling industry in Great Britain. It licenses the operation of casinos, bingo, gaming machines and lotteries (on site, telephone and internet gambling) and is a supervising authority under the Money laundering Regulations 2007. Where necessary it revokes licences and prosecutes illegal activity. An example of the use of covert techniques is to investigate and close down

unregulated poker clubs (which do not afford adequate protection against the involvement of children, intimidation,, extortion and cheating).

Gangmasters Licensing Authority

The Gangmasters Licensing Authority 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/prosecutes those without a license. Communications data can link unapproved gangmasters to the migrants they are exploiting. It is important that the problem is addressed by taking effective action against both labour providers and labour users that exploit illegal migrant workers.

Health and Safety Executive

The HSE is the enforcement authority for most work-related health and safety legislation. It investigates and prosecutes offences which involve the creation of serious risks to people's health and safety such as poisonings, explosions from faulty domestic gas installations, major chemical incidents (such as the December 2005 Buncefield oil depot explosions), movement of dangerous goods and construction site injuries etc. HSE obtains communications data in order to trace and investigate individuals or businesses whose activities may be putting people at risk of serious harm or where mobile phone use may be among the causes of an incident.

HM Revenue and Customs

HMRC uses communications data in connection with policing/assuring a wide range of UK revenues, taxes and duties as well as protecting the public at the border by combating the smuggling of prohibited, restricted and duty payable items. This is necessary to tackle the avoidance of millions of pounds of duties and taxes on goods and attacks on the self-assessment and tax credit systems, where organised crime gangs with false identities use multiple claims to obtain large repayments. HMRC also carries out investigations in the interests of national security (for instance enforcing trade sanctions and embargoes, countering the trafficking of weapons of mass destruction and in support of Project Cyclamen – a cross-Departmental initiative to screen for the illicit importation of radioactive materials).

Home Office - UK Border Agency

The Home Office UK Border Agency (UKBA) uses communications data to tackle organised immigration crime and attempts to undermine the integrity of border control. In addition, the merger of the former Border & Immigration Agency with UK Visas and HMRC detection work at the borders to create UKBA has resulted in a broader remit of responsibility for the Agency that now includes customs offences. UKBA has a lead role in investigating border related crimes, including trafficking and the smuggling of people, drugs and criminal cash, as well as illegal working cartels, asylum abuse, fraud, deception and other immigration offences. The Agency also now plays a vital role in the prevention and detection of prohibited or restricted goods such as firearms or paedophile material. Increasingly sophisticated methods to facilitate illegal entry and organise the trafficking of people include the use of communications services to plan, conceal and undertake illegal conduct. The UK Border Agency has also used communications data in anti-corruption investigations against Border Agency staff suspected of conducting or colluding in immigration crime.

The UK Border Agency Detention Services serves the public by escorting and holding people detained under immigration law and by assisting in the removal of those not entitled to stay in

the UK. Detainees in immigration removal centres are allowed access to personal mobile phones and the internet whilst in detention. Whilst such access is restricted and policed by staff, it may be abused. In particular, given the availability of landline telephones throughout detention establishments, it is suspected that mobile phones are used for the purpose of criminal activity including drug movements, escapes, terrorist associations and grooming of minors by paedophiles. Communications data will provide an enhanced intelligence picture to assist in the prevention and detection of crime.

The UK Border Agency provides support, accommodation and financial help for asylum seekers whilst their claims for asylum (and appeals of asylum decisions) are being considered. Proportionate and restricted access to communications data is required to assist the UK Border Agency to investigate individuals suspected of making fraudulent claims and stop benefit cheats who steal from the genuinely deserving.

Independent Police Complaints Commission

The IPCC took over in 2004 from the Police Complaints Authority to oversee the handling of public complaints of misconduct by the police and other law enforcement bodies. Its independence from law enforcement agencies means it needs its own investigatory powers. Where someone dies as a result of contact with a law enforcement agency the agency itself is required to notify the IPCC which conducts the investigation on behalf of the coroner. It is these cases where the use of communications data can help identify the victim and his location at the time of the incident and enables family or friends to be contacted to establish his state of mind at the time.

Information Commissioner

The Information Commissioner is the independent supervisory authority responsible for enforcing the provisions of the Data Protection Act 1998, the Freedom of Information Act 2000 and the Privacy & Electronic Communications Regulations 2003. Personal information has a financial value and can be traded for criminal purposes to the detriment of the individual whose data is stolen and misused, and for society at large. It is a criminal offence under the 1998 Act to unlawfully obtain, disclose, sell or offer to sell personal information. The Commissioner's Office 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.

Intelligence Agencies (GCHQ, the Security Service and the Secret Intelligence Service)

The intelligence agencies use communications data in their operations involving national security (for example identifying persons within the UK and elsewhere who conspire to harm the public), in support of the prevention and detection of serious crime and in the interest of the economic well-being of the UK.

The Security Service protects UK from threats to national security (including terrorism and espionage) and helps counter proliferation of weapons of mass destruction. Its covert intelligence investigations enable it to identify, assess and counter these threats.

SIS collects foreign intelligence on behalf of the UK and has a global covert capability to promote and defend the UK's national security and economic well-being. It supports the Security Service's responsibilities and represents its interests with co-operating foreign intelligence agencies.

GCHQ collects intelligence from communications and related sources and provides information assurance advice to help keep Government communications and information systems safe from hackers and other threats.

Local Authorities

353 local authorities in England, 22 in Wales, 32 in Scotland and 26 in Northern Ireland are able to use service use and subscriber data in order to prevent or detect crime or disorder in connection with their statutory functions. Many of these functions are their sole responsibility.

Examples of investigations where covert techniques enable local authorities to trace investigations back to a source individual at a specific address and offer evidence against them in legal proceedings include:

- trading standards (eg action against loan sharks and rogue traders, car fraud, consumer scams, deceptive advertising, counterfeit goods, unsafe toys and electrical goods);
- enforcement of anti-social behaviour orders and legislation relating to unlawful child labour;
- housing/planning (eg intervening to stop and take remedial action against unregulated and unsafe building, breaches of preservation orders, cases of landlord harassment);
- benefits fraud (eg housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations, council tax evasion); and
- environment protection (eg action to stop large-scale waste dumping, the sale of unfit food and illegal 'raves').

The advantages of being able to use communications data to help criminal investigation especially in trade and consumer scams is becoming more important with the growth of the internet and distance selling. Many transactions are now done without buyer and seller coming into contact and often the only way of linking offenders to these transactions is by communications data.

Ministry of Defence Police

The Ministry of Defence Police provide a nationwide, armed guarding role at defence sites requiring a high level of security, protecting against the sabotage of assets. This includes guarding Britain's nuclear deterrent. Communications data assist them in carrying out their duties, which include the prevention and investigation of defence crime, fraud and corruption.

Ministry of Justice

The Ministry of Justice National Offender Management Service is responsible for holding prisoners securely, reducing the risk of prisoners re-offending and providing safe and well-ordered detention establishments. It uses communications data to investigate offences involving staff corruption and to prevent and detect crime, in particular the supply of illegal drugs in prison establishments. There has been considerable growth in the smuggling of mobile phones into prisons which are used to organise the supply of contraband into prisons and the commission of other offences outside of prisons, for example the intimidation of witnesses.

NHS Services

The three NHS counter fraud services (England/Wales, Scotland and Northern Ireland) use communications data to tackle fraud and corruption within the NHS - either by practitioners, patients, staff or contractors - which cheats taxpayers and takes valuable resources away from

patient care. The England/Wales body - the Counter Fraud and Security Management Services Division of the NHS Business Services Authority - also investigates breaches in security which put patients and NHS assets at risk. NHS fraud can be committed by practitioners, patients, staff and contractors. Since 1999, NHS counter fraud work has brought 482 successful prosecutions and recovered over £57m from fraud and unlawful action in the NHS.

Northern Ireland Office – Prison Service

The Northern Ireland Prison Service is responsible for holding prisoners securely, reducing the risk of prisoners re-offending and providing safe and well-ordered detention establishments. It requires communications data to investigate offences involving staff corruption in prisons and to prevent and detect crime, in particular the supply of illegal drugs in prison establishments. This will bring prisons in Northern Ireland into line with the rest of the UK.

Office of Communications

The Office of Communications is the independent regulator and competition authority for all the UK communications industries, with responsibilities across television, radio, telecommunications and wireless communications services. It acquires communications data to investigate the location and operation of illegal radio broadcasters under the Wireless Telegraphy Act 2006. This essentially means people who buy equipment from the internet and set up hidden studios to broadcast at any frequency in the radio spectrum regardless of whether that frequency is already licensed to a legitimate station. These unlicensed operators pay no taxes, provide unfair competition, interfere with legitimate broadcasters and their audiences, and disrupt vital safety of life emergency services.

Office of Fair Trading

The Office of Fair Trading is the UK's consumer and competition authority. It obtains communications data in the course of investigating breaches of competition law under the Competition Act 1998 and the Enterprise Act 2002, and misleading or aggressive business practices under the Consumer Protection from Unfair Trading Regulations 2008. This includes tackling cartels, which are among the most serious forms of anti-competitive behaviour and which could result in significant detriment to UK business and consumers. It also includes investigating serious breaches of consumer law, for example rogue traders, and scams which exploit low-cost, mass-marketing techniques to target recipients. It is estimated that UK consumers lose up to £3.5 billion a year to these, including bogus lotteries, pyramid schemes and deceptive premium-rate prize promotions.

Office of the Police Ombudsman for Northern Ireland

The Office of the Police Ombudsman for Northern Ireland uses communications data to help discharge its responsibility to investigate complaints of criminality and serious misconduct made against law enforcement agencies. These include the Police Service of Northern Ireland, Belfast Airport Police, Harbour Police and MOD Police operating in Northern Ireland. It is important that it retains its own investigative powers so that its investigations are independent of the police services it is investigating.

Pensions Regulator

The Pension Regulator is responsible under the Pensions Act 2004 for the proper running of occupational pension schemes. The Regulator enforces employers' responsibilities to offer proper workplace pensions without penalty and to maintain the system of payments as

arranged. RIPA authorisations allow tracking of illegally transferred funds from genuine company pension arrangements into bogus schemes by unscrupulous individuals operating on the internet (so-called 'pension liberators'). Sanctions include disqualifying pensions' scheme trustees, imposing fines and appointing new trustees to pension schemes in difficulty.

Police forces

The police use communications data for the purpose of preventing and detection of crime across a broad range of policing areas, for example to establish the whereabouts of a person who has been kidnapped and whose life is threatened, research what communications were made or received by the victim in a murder investigation, assist victims and witnesses to determine or corroborate certain facts and assist the police to assess alibis. The police also rely on other statutory purposes under RIPA to acquire data to assist them in general policing activities which include identifying the whereabouts of missing children, establishing a person's next of kin, and assisting HM Coroner to establish the facts that lead to a person's death. Communications data has helped secure convictions for terrorist offences and serious crimes, including many murders.

Ports Police (Dover and Liverpool)

The Port of Dover Police and the Port of Liverpool Police are responsible for law enforcement and the security of passengers and staff at their respective ports. They provide round the clock policing, investigative and prosecuting services to the owners, tenants and users of shipping premises, ferry and cruise terminals. Each year some 16 million people pass through Dover, and 700,000 through Liverpool. Communications data enables both forces to secure evidence necessary to prevent and detect criminal offences associated with commercial and passenger services in the docks' area, and to undertake their counter-terrorism and public safety functions.

Postal Services Commission

The Postal Service Commission is the independent regulator for postal services in the UK which acts to protect the interests of the postal industry and its users. It acquires communications data to investigate breaches of the Postal Services Act 2000. These relate to offences of unauthorised postal operations, including unlawfully collecting, conveying and delivering mail without a licence and interfering with mail (e.g. intentionally delaying or opening a postal packet) in the course of its transmission.

Royal Mail

The Royal Mail Group Ltd acquires communications data in its capacity as universal postal service provider. This enables it to fulfil its long standing role of investigating criminal offences such as theft of and/or conspiracy to steal mail in course of transmission by post, including mail containing passports and identity information as well as financial items and valuables, postage evasion fraud and people selling stolen goods on the internet. Communications data can help identify and locate the people using the stolen items.

Scottish Crime and Drug Enforcement Agency

The SCDEA prevents and detects serious and organised crime as it affects Scotland at a national and international level. It uses communications data to identify, strip away assets, seize money and help imprison those involved in serious and organised crime, particularly drug trafficking.

Serious Fraud Office

The SFO was set up by the Criminal Justice Act 1987 to investigate and prosecute serious or complex fraud in cases where monies at risk are at least £1m, where there is a national concern or a significant international dimension or where the investigation requires highly specialist skills. The SFO operates mainly in the fields of market manipulation, fraudulent share dealing and 'dial through', concealed frauds. Sums 'at risk' in the 60 cases it investigated in 2007/08 were estimated at £4.8 billion. 65% of SFO investigations have international dimensions, and a further £30 billion of 'at risk' sums were investigated in 2007/08 responding to overseas requests for mutual legal assistance. The SFO's work reduces fraud and the cost of fraud. This enables confidence in the UK's business and financial institutions to be maintained.

Serious Organised Crime Agency

SOCA, which includes the Child Exploitation and Online Protection Centre, uses communications data, which includes traffic data, to assist investigations into serious and organised crime. This covers a wide range of activities and individuals and includes trafficking of class A drugs, organised immigration crime and fraud, hi-tech crime, counterfeiting currencies and serious robberies involving firearms. In the internet environment, it includes protecting children by identifying sex offenders undertaking grooming activities and tracking down convicted sex offenders who have failed to notify the authorities of their abode. SOCA is responsible for facilitating the lawful acquisition of communications data to assist investigations and operations spanning international borders which are coordinated through Interpol.

8. Consultation outcome

8.1 A public consultation which took place from 17 April to 10 July 2009 invited views on, amongst other things, all relevant public authorities listed under RIPA, the ranks of officers able to authorise RIPA techniques, and the statutory purposes for which techniques can be used. Of the 222 responses received, most were broadly supportive of the Government's view that the public authorities listed in Schedules 1 and 2 of the draft Order had a continuing well-founded need to authorise the acquisition of communications data under RIPA when necessary and proportionate to do so. Only a handful of responses suggested greatly reducing the number of public authorities able to authorise the acquisition of communications data under RIPA, but there was no consistency in which should be removed and none provided convincing reasons for removing them.

9. Guidance

9.1 The Home Office statutory code of practice made under RIPA on the acquisition and disclosure of communications data was revised in 2007 following public consultation. Guidance is also provided by the Interception of Communications Commissioner's Office, which also has the statutory responsibility to oversee the acquisition of communications data under RIPA. Accredited training for public authority single points of contact is provided by the National Anti-Fraud Network and the National Policing Improvement Agency.

10. Impact

10.1 The impact on business, charities or voluntary bodies is nil.

10.2 An Impact Assessment has not been prepared for this instrument

11. Regulating small business

11.1 The legislation applies only to public authorities.

12. Monitoring & review

12.1 The Government will keep under review the operation of this legislation, including:

a) through the independent inspection and oversight by the Interception of Communications Commissioner (who also has statutory responsibility keeping under review the acquisition by public authorities of communications data under Chapter II of Part I of RIPA); and

b) through the Investigatory Powers Tribunal which is made up of senior members of the judiciary and is independent of Government and has full powers to investigate and determine any proceedings or complaints falling within its jurisdiction.

13. Contact

13.1 Tony Cooper of the Covert Investigation Policy Team at the Home Office, 2 Marsham Street, London SW1P 4DF (telephone 020 7035 1218; e-mail tony.cooper3@homeoffice.gsi.gov.uk) can answer any queries regarding the instrument.