

Written evidence submitted by Chris Farrimond, National Crime Agency, Simon Grunwell, HM Revenue & Customs, and Richard Berry, National Police Chiefs Council (IPB 63)

April 2016

Further to the informal briefing that you received at the NCA on the 22nd March 2016 and public evidence given by NPCC, NCA and HMRC on the 24th March we enclose our written evidence for the commons committee stage of the IP Bill covering:

- clarification of what legislation currently governs Law Enforcement's use of the powers that are being refreshed in the IPB;
- common misconceptions in respect to Law Enforcement's use of investigatory powers and the provisions that the IPB make for Law Enforcement;
- the Law Enforcement authorisation process for the three powers of targeted Communications Data (CD), Equipment Interference (EI) and Lawful Intercept (LI) as they currently stand under existing legislation; and
- examples of the use of EI and CD for law enforcement investigations into a range of criminal activity.

For further reading we would like to draw your attention to the written evidence that we provided to the Joint Scrutiny Committee that is published on the Government website (<http://www.parliament.uk/draft-investigatory-powers>) and includes detail on:

- **technology and the impact on investigations** (the issue of how the internet and communications has changed);
- the draft **Bill provisions for CD** (as it stood in the draft Bill prior to introduction and the JSC recommendation which has resulted in the inclusion of a 4th purpose of Internet Connection Record (ICR) use. As described at the informal briefing the fourth purpose is crucial in providing a wider picture of a suspect's activity / a missing person's last actions online that could help trace them);
- **real life examples of the threat and operational cases** where we have used CD or need improvements to CD capability in the online space to assist with investigations; and

- data from National Policing on **the use of CD** describing the **types and range of cases that CD is used in**.

The IPB updates existing legislation and provides a new obligation on service providers to retain Internet Connection Records

All powers available to law enforcement under the IPB are currently available under existing legislation. The only exception to this is in relation Internet Connection Records (ICRs), where it is proposed that a new obligation should be placed on service providers to maintain records of ICRs. This will enable law enforcement to keep pace with developments in technology in the digital age. The grid below explains how these powers read across from old to new legislation.

Fig 1. IPB Powers Comparison to Existing Legislation

Power	IPB Part and Section	Current Legislation	What's New
LI	Part 1 Sections 2-8 and Part 2 Chapter 1-3	RIPA Wireless Telegraphy Act 2006 Codes of Practice	<ul style="list-style-type: none"> • Increases the length of serious crime warrants to 6 months in line with warrants for national security. • Judicial Commissioners authorisation prior to the issuing of a warrant – double lock.
CD	Part 1 Section 9 & 10, Part 3 & 4	Data Retention and Investigatory Powers Bill 2014 Acquisition and Disclosure of Communications	<ul style="list-style-type: none"> • Provide for the retention by CSPs of ICRs • New definitions of communications data (introduction of entities and events data) • Judicial authorisation in relation to acquiring communications data to identify or confirm a journalistic

		Data: Codes of Practice RIPA	source.
EI	Part 1 Sections 11 & 12, Part 5	RIPA Section 93 of the Police Act 1997 Codes of Practice	<ul style="list-style-type: none"> • Introduces a new warrant regime for authorising EI activity with robust safeguards • Provides a statutory basis for authorising EI activity to prevent death or injury. • Provides Judicial Commissioner approval of warrants in order to authorise EI activity.

Each of the existing powers referred to above is subject to an authorisation regime that requires an applicant to demonstrate to the authorising officer that the investigative method proposed and the intrusion into privacy required is both necessary in order to achieve a lawful purpose and a proportionate means of doing so. The applicant will need to consider any collateral intrusion that may arise as a result of using the investigative method and explain how it will be minimised. They will also have to consider whether there are other less intrusive techniques that could achieve the same outcome.

In making the application the applicant must provide sufficient detail to enable the authorising officer to make an informed decision, balancing up what will be achieved against the intrusion into privacy and the authorising officer must record their decision and rationale for making the decision, for which they are then accountable.

This process is explained in greater detail in Annex A

Each of these applications and authorities is retained and is available for inspection by the relevant oversight body at a later date.

Human Rights Act principles are therefore already embedded in existing authorisation regimes and we anticipate that these same robust and auditable processes will be used to ensure proportionate use of the powers when their deployment is necessary in order to achieve a lawful purpose.

Communications Data

Service providers retain Communications Data and under the IP Bill would still be responsible for doing so. **Law Enforcement will only access this data using targeted enquiries when it is necessary and proportionate.**

CD is stored by the relevant Communication Service Provider (CSP). Law Enforcement request targeted access to this data by following a strict authorisation process which sets out what data is required and why. If an authorising officer decides that a request is necessary and proportionate the request is approved and specific data obtained from the CSP. See **Annex A:** Necessity, Proportionality and Collateral Intrusion: Explained and **Annex B:** Law Enforcement Communications Data Authorisation Process.

Communications Data is a key tool for policing, used daily across a whole spectrum of threats and crime types from cyber bullying, to online fraud and CSE cases.

ICRs

As more communications that would traditionally have been sent through traditional telephony are now internet-based, the same information that would have been accessible through CD will increasingly only be available through ICRs. For instance, text messages are now routinely sent by internet-based communications. Without access to ICRs the intelligence that can be gathered from CD will continue to decline and Law Enforcement will be unable to keep pace with criminal use of communications.

A suspect's ICRs may reveal information about that person's interests and habits online, since in today's society more of our lives are lived online. However, this should be balanced against the reality that the internet enables more crime to be organised or committed online, with a greater degree of anonymity than traditional phone calls or face to face meetings.

The advent of the internet and social media has seen an increase in 'cyber' bullying, stalking, harassment and online child abuse. Equally, traditional crimes such as fraud can be committed at scale and drugs or human trafficking arranged online without perpetrators needing to know or meet one another, eroding the opportunity for law enforcement to identify and evidence crime. Law Enforcement powers need to be updated to ensure that crimes in the age of widespread digital communications can still be investigated.

The use of CD and therefore ICRs for lower levels of crime or volume crime is key to investigating cases of harassment, grooming, sextortion, anti-social behaviour, theft, domestic abuse and stalking. These crimes are often precursors to serious crimes but do not, themselves, meet the serious crime definition in the Bill. In such cases, and others, ICRs may often be the only investigative lead.

Fig 2. Crime Types that use Communications Data to investigate offences.



See **Annex E** for examples that explain how CD is used in investigations across the spectrum of crime types and how the different purposes of ICRs would assist with furthering investigative leads.

Requests for ICRs, like all CD, will only include the data that is necessary in a specific case. So if ICRs are only needed for a short window of time, for example to ascertain whether someone has been using the internet while driving, then that's all that will be sought.

An ICR is not a record of full web browsing history. If the Bill is passed in its current form, ICRs place an obligation on UK service providers to retain the required data. ICRs will enable law enforcement to reach the 'front door' in an investigation by either resolving IP addresses to a device and therefore to a suspect or victim, or enabling investigators to request data about a suspect or victims activity online that can provide investigative leads which enable further enquiries. If further information is required from the services that have been identified as being used by a suspect or victim, other legal instruments will be required such as a production order or result in further Communications Data requests.

ICRs for IP Address Resolution helps to identify potential suspects and victims. CD provides one type of intelligence, they are often the **starting point to investigations but seldom used in isolation.** With many communications taking place online an IP address is often the only lead available to law enforcement to investigate a suspected case of abuse. The NCA receive approximately 1300 to 1500 referrals a month from the National Centre for Missing and Exploited Children (NCMEC) relating to indecent images of children. A sample of data (6025 referrals) found 14% to be unresolvable without the additional data that would be retained by the provision of ICRs under current data retention laws. **This is the equivalent to 862 cold cases because data that would enable IP Address Resolution** is not consistently retained by all service providers.

Equipment Interference

Law Enforcement Agencies (LEAs) currently conduct activity which will in future fall within the definition of Equipment Interference (EI). This is presently authorised under the **Police Act 1997** for the prevention and detection of serious crime and authorised at Chief Constable Level with Judicial oversight (OSC) using a 'double lock' authorisation process.

The Bill does not provide any new EI powers to LEA's, however it does provide a clearer legislative framework for authorising EI, with improved safeguards and oversight. The same law enforcement agencies undertake the same activity: this is not an expansion of police powers.

EI is critical in supporting LEA's investigation and prevention of serious and organised crime on an international, national and local level. These crimes are varied and include sexual abuse of vulnerable individuals, drug trafficking, fraud, people trafficking and other organised crimes and terrorism offences.

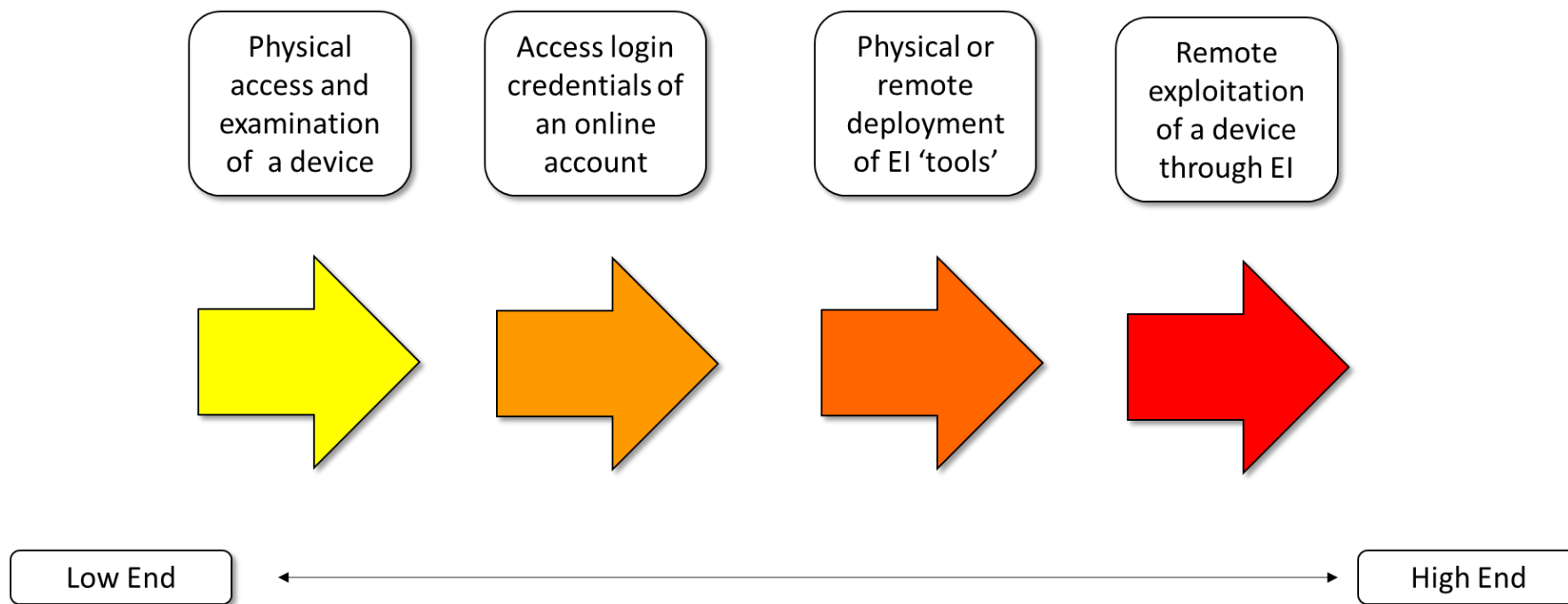
EI may also be used in order to prevent death or harm to vulnerable people where there is no associated serious crime. This could be in relation to a missing child. For example, a police force may wish to use a child's password to access their social media account if they are missing and thought to be at risk. This type of activity will only be used in exceptional circumstances. The Bill will ensure that only a select group of law enforcement agencies can continue to carry out this activity under the safeguards and oversight set out in the Bill.

EI warrants will authorise the interference with equipment to obtain communications, equipment data or other information. The definition of EI covers a wide range of technical capabilities that enable LEA's to gain targeted access to data; ranging from physical access and examination of a device, access to login credentials of online accounts, up to remote exploitation of a device.

Not all LEA's will have access to all EI capabilities. EI will only be authorised where it is proportionate for the warrant to be issued to the applicant LEA. Considerations include whether the applicant has sufficient capabilities, whether the technique has been adequately tested and experience, whether there are sufficient safeguards to protect the technique and whether it would be more appropriate for another LEA to obtain the warrant. Accordingly, the use of t advanced and

sensitive techniques will be restricted to selected LEA's and specialist units. Agencies with specialist units and suitably trained Officers.

Fig 3. Range of Equipment Interference Capabilities



Annex D explains the current oversight and authorisation regime for Part III of the Police Act, including the activities that are classified as Equipment Interference in the IPB.

Examples of Equipment Interference used by LEA's

Example A

A law enforcement operation was enacted to tackle an organised criminal group involved in large scale drug supply and related money laundering offences. A member of the OCG was identified as pivotal to the operation, however due to their status and previous criminal history the use of conventional police tactics such as surveillance were not viable.

A plan was devised and executed that enabled the subject's mobile phone to be covertly downloaded. The information from this download was used to identify other members of the network and devices or phone numbers used by the group.

The activity enabled the identification of other criminals and provided a number of other lines of enquiry and opportunities to frustrate and counter the activity of the organised criminal group.

Example B

A law enforcement operation commenced to locate and recover a 14 year old girl who was known to social services who had been reported missing from her home and was considered to be at risk of sexual exploitation.

Through the use of equipment interference police were able to identify an electronic device she was using. Additional equipment interference and other intelligence identified a hostel premises in London where the girl was suspected to be staying, however, when police attended the premises, the girl had left having vacated the hostel earlier that day.

Further equipment interference was undertaken which enabled police to identify another premises in a different area of London where the girl was found in the company of a known criminal. The girl was recovered safe and well and returned to her family.

Example C

The NCA used targeted equipment interference techniques against an advanced cyber-crime group and those laundering the proceeds of their criminality.

These cyber criminals target individuals in the UK and worldwide, infecting victim computers with financial Trojans and malware, which allows them to fraudulently transfer monies from victim accounts. The widespread use of this financial Trojan has been reported as having enabled attackers to steal hundreds of thousands of pounds per attack.

The criminal network is sophisticated in its operations, including using encrypted means of communication to avoid detection.

An equipment interference technique was deployed to capture the key strokes of members of the criminal network. This provided information that would not have been obtained through any other conventional means. The deployment of this equipment interference technique provided insights into the activities of the individuals, thereby informing the investigative strategy.

Example D

The NCA used equipment interference techniques to target a sophisticated organised cyber crime network. The criminal organisation deployed persistent malware onto individuals' devices and used this to harvest the banking details of its victims, allowing criminal associates to steal monies from victim accounts.

By way of advanced equipment interference techniques, the NCA was able to infiltrate the organised crime group. This provided the NCA with vital information as to how the criminal network operated and also enabled the NCA to view / identify stolen data. By sharing this information with partners and engaging with relevant third party organisations, the NCA was able to mitigate the threat and protect potential victims.

The estimated collective loss to the UK public resulting from the actions of this particular organisation is believed to be in the tens of millions of pounds.

Lawful Intercept

The IPB maintains the current capability of Intercepting Agencies to conduct targeted interception to prevent and detect serious crime; creating a 'double lock' authorisation process requiring the involvement of both a Secretary of State and a Judicial Commissioner.

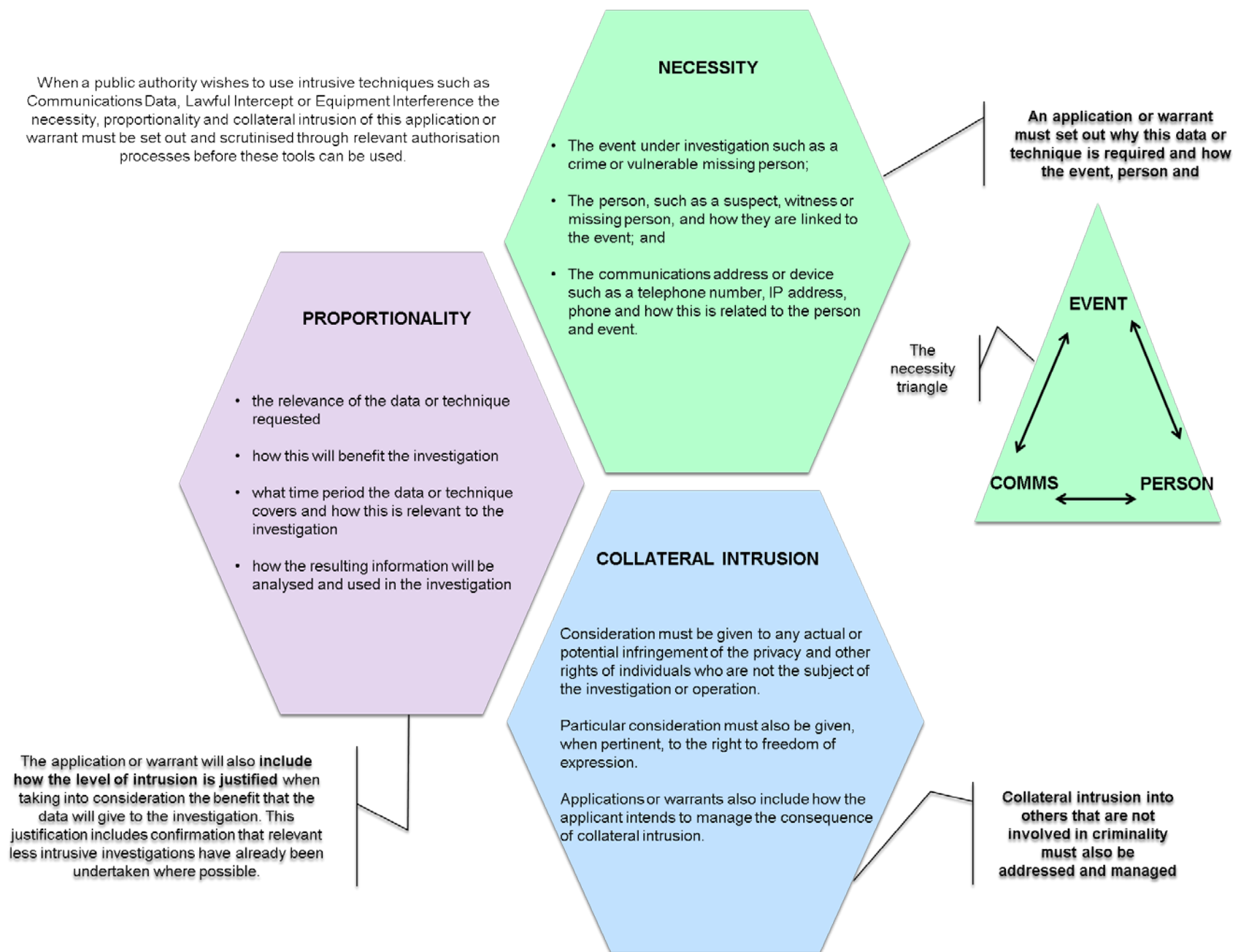
Law Enforcement Agencies (LEAs) will continue to use interception in relation to the investigation of a wide spectrum of serious criminal activity which will include situations that are time critical, unusual or involve threats to life, and which require immediate action.

For example where a kidnap takes place and / or there is a threat to the life of an individual, law enforcement must be able to respond quickly and dynamically to save lives. In this type of situation, Law Enforcement Agencies may seek to obtain a thematic warrant, allowing them to respond effectively and quickly to the changing and dynamic nature of a developing situation.

LEA's continued use of a thematic warrant in these type of circumstances is essential in maintaining their capability to effectively deal with these types of situations. It should also be noted that a thematic warrant is also subject to the 'double lock' process and will only be issued if its use is considered to appropriate and is both necessary and proportionate in the specific circumstances.

Annex C explains the current Lawful Intercept authorisation procedure and oversight regime.

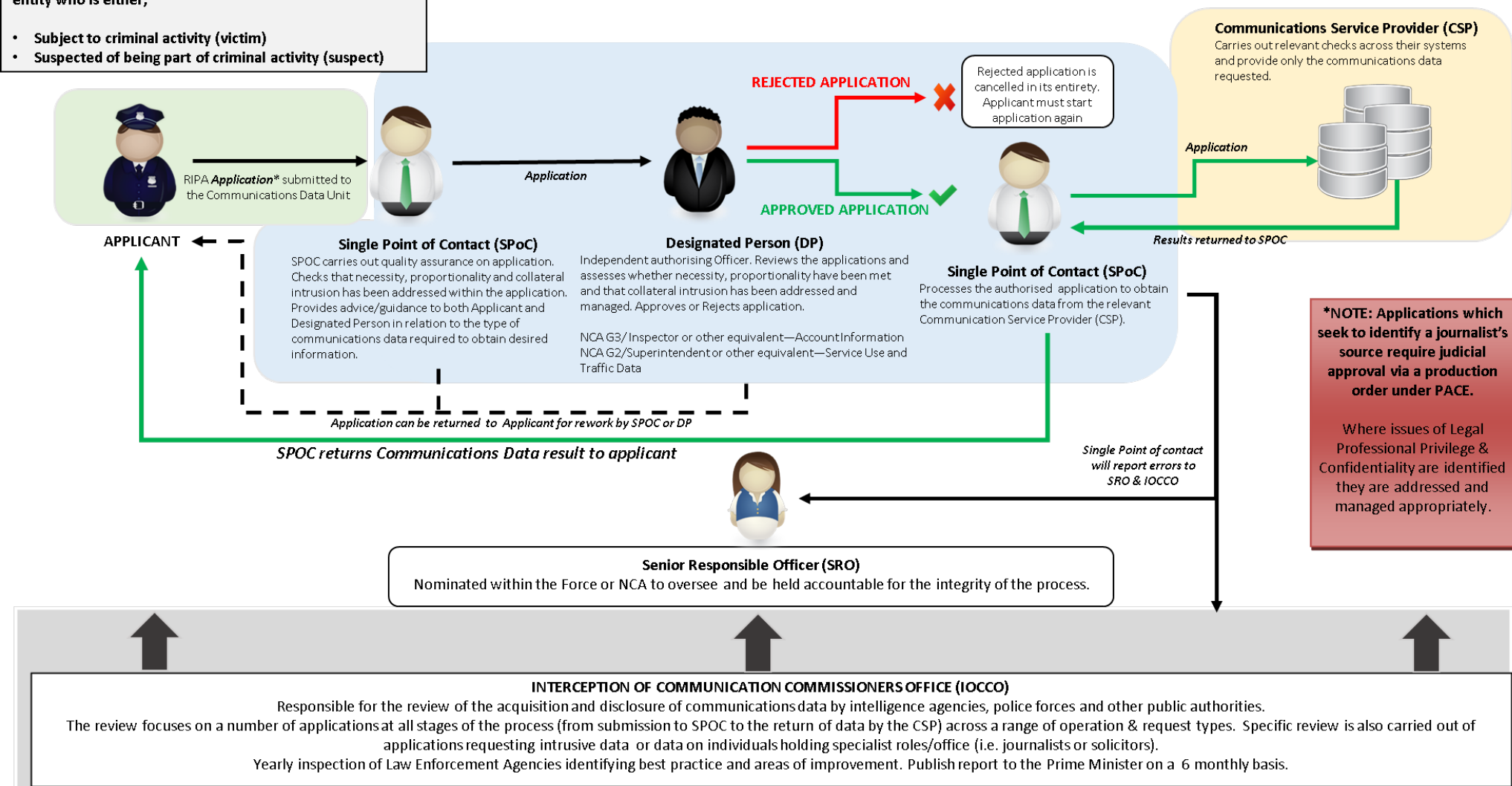
Annex A: Necessity, Proportionality and Collateral Intrusion: Explained



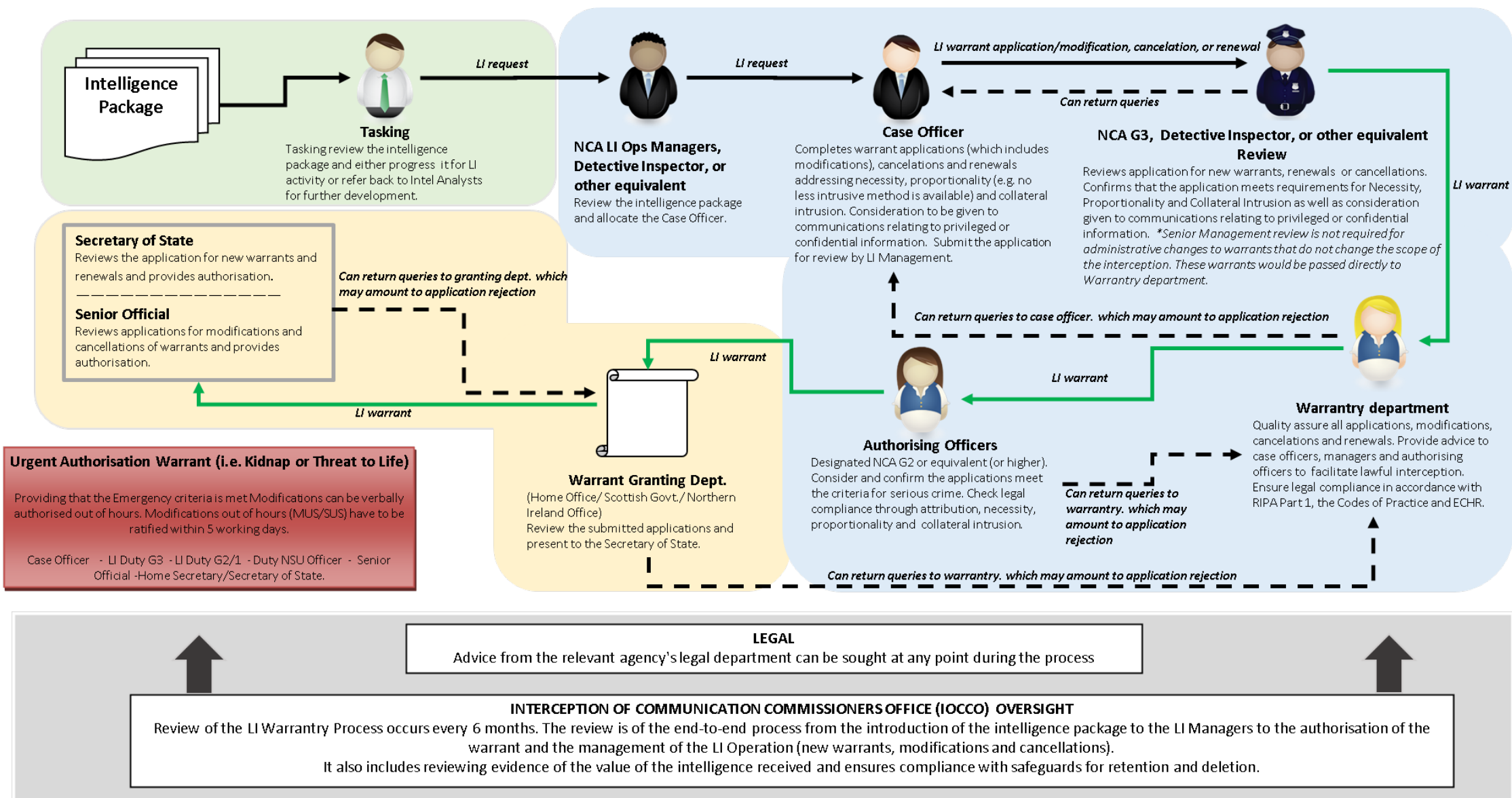
Annex B: Law Enforcement Communications Data Authorisation Process.

Law enforcement can only access communications data when they have a seed of information connected to an entity who is either;

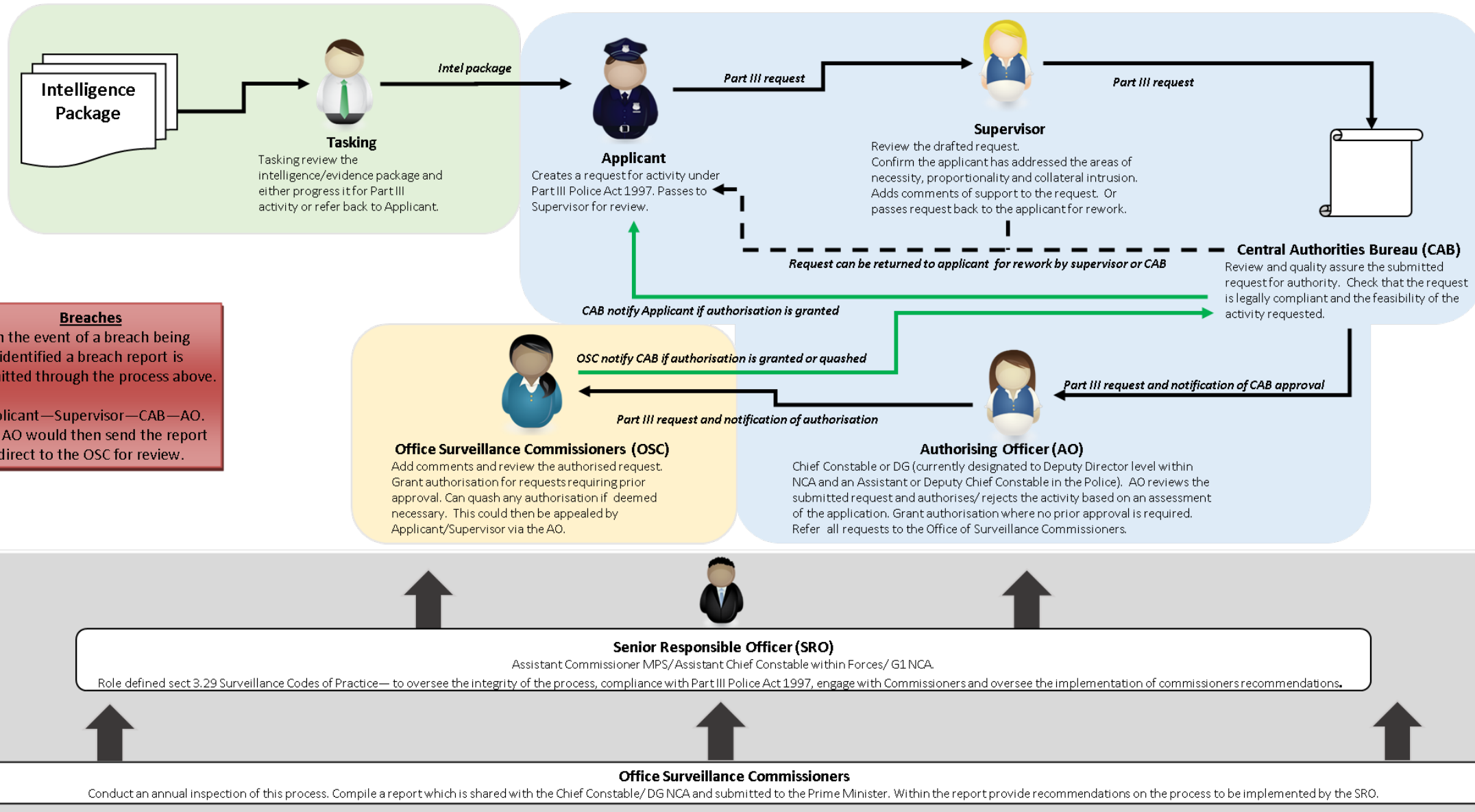
- Subject to criminal activity (victim)
- Suspected of being part of criminal activity (suspect)



Annex C: Law Enforcement Lawful Intercept Authorisation Process.



Annex D: Law Enforcement Property Interference Authorisation Process.



Annex E: Operational Examples of the use of CD and application to ICRs.

Under current Bill provisions, the authorisation of ICR retrieval is not permissible unless the **purpose of obtaining the data is to identify:**

- (a) **which person or apparatus is using an internet service** where—
 - (i) the service and time of use are already known, but
 - (ii) the identity of the person or apparatus using the service is not known,
- (b) **which internet communications service(s)** is/are being used, and when and how it is being used, by a person or apparatus whose identity is already known, or
- (c) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves **making available, or acquiring material whose possession is a crime**
- (d) Which **internet service** is being used, and when and how it is being used by a person or apparatus, whose identity is already known.

The following nine examples explain how CD is used in investigations across the spectrum of crime types and how the different purposes of ICRs would assist with furthering investigative leads.

Fraud - ICR Purpose 'A' - Which person or apparatus is using a specified internet service ?

1. Henry has £50,000 savings and wants to buy a property in Malta. He subscribes to a Maltese property circular and receives an email from **valettainvestments@securmail.com** regarding an investment opportunity in the island's capital. He exchanges emails with Valetta Investments 'representative' and agrees to meet at a central London Hotel where he hands over a cheque for his savings.

2. He does this after online research which confirms that there is indeed a complex being built by a company called Valetta Investments on the island. Two weeks later however he has heard nothing from the representative and contacts the real company directly, only to discover that the email account, and representative, are false. He reports the fraud to police.

4. Historic ICRs records are examined to identify individuals accessing the securmail server(s) at or about the dates / times when the emails were sent to / from valettainvestments@securmail.com to Henry. A broadband line is identified as consistently accessing the securmail servers at these corresponding times, leading to the arrest of the 'representative' and recovery of Henry's savings.

3. Police recover all emails from his computer. Securmail are a niche overseas based supplier of encrypted email services. Part of the service includes the deletion of customer IPs from the email 'header' leaving no traceable features except date and time of sending.

Online Harassment – ICR Purpose 'D' - Which internet service(s) have been used ?

1. Following the break up of her relationship the victim received threatening emails from successive 'disposamail.com' email accounts (This service offers a disposable '24Hr' email account to users)

Some of the threatening emails included photographs of torture victims. The victim blocked 'disposamail' accounts from her inbox.

2. The victim was then notified by friends that a socialmedia.com account had been set up in a name similar to her own, and with her photo. This account was being used to post abusive and racist comments about some of the victim's friends on socialmedia.com.

4. Historic ICRs for the ex-partner's phone are obtained. These confirm repeated access to bestproxy.com. Temporal and data size comparison with the threatening emails / access to socialmedia.com confirm suspicions. Connections to the torture victim website are also evident. The ex-partner is arrested and, faced with the facts, admits the offences.

3. Enquiries identify that the email / socialmedia accounts were set up / accessed via 'bestproxy.com,' hiding the users IP address behind a commercial 'proxy' service.

Officers also locate the website hosting the torture victim photos. Suspicion exists that the victim's ex-partner is behind the abuse.

Human Trafficking for Prostitution - ICR Purpose 'A' - Which person or apparatus is using a specified internet service ?

1. A UK based Albanian OCG are trafficking women to the UK for the purposes of enforced prostitution.

The OCG advertise for victims in social media in Albania and Serbia, purporting to employ staff for the service industry in the UK, complete with board and lodging.

2. Victims are then directed to a fake Albanian 'employment' site where arrangements are made over a private chat facility.

Once in the UK the victims are forced into the sex trade in order to pay off extortionate fees associated with their transport to, and facilities provided in the UK.

4. Historic ICR queries through UK CSPs are conducted to identify any customer(s) accessing the Albanian employment site at specified times when the CII was in communication with OCG members on the site.

This information enables the investigating team to identify OCG members through follow on investigations.

3. A victim has escaped and alerted police. She has details of the false Albanian social media / employment website but does not know where she was held. This has however enabled a covert internet investigator (CII) to engage the OCG via the employment site, posing as Albanian female seeking work in the UK.

Locating a Vulnerable Missing Person – ICR Purpose 'D' - Which internet service(s) have been used ?

1. Amy is a impressionable 16 year old girl with some learning difficulties.

She disappears from home early one morning while her parents are asleep. Her parents try ringing her mobile but it is switched off. They inform Police.

2. Traditional telephony Communications Data requests reveal no useful calls or texts relevant to Amy's whereabouts.

The phone appears to have been switched in the vicinity of the family home earlier that morning.

4. Historic ICRs are requested for Amy's mobile phone for the preceding 24 hour period. This shows connections to theTrainline.com and the website of a band, The Blue Monkeys. Open Source research identifies that the band are playing at a central London venue that evening. Officers visit the venue where Amy is located safely.

3. Traditional 'Missing Person' enquiries - with friends and at local bus / taxi firms prove negative.

Review of available CCTV shows Amy boarding a London bound train however. Enquiries confirm that Waterloo was her final destination but CCTV footage there is insufficient to trace Amy further.

Tracing a murder suspect - ICR Purposes 'A & D' - Which person or apparatus is using a specified internet service / which internet services have been used ?

1. Peter, a drug trafficker, is wanted for murder following a fight in a nightclub where he stabbed another customer. He is well known at the club and knows he will probably be linked to the offence. He moves to Scotland to live with a friend, destroying his mobile phone and buying a new pre-pay unregistered device.

2. Peter moves his comms 'online,' contacting associates through a 'clean' intermediary advising them to install a specified instant messaging App called RightNow. Officers do identify Peter as a suspect and determine that his known mobile number has been switched off. Traditional enquiries fail to identify a new number.

4. Officers make a further ICR query to identify a phone which came live within a week of the attack and which visits all 5 websites. A mobile service provider returns a result for a phone which first registered two days after the attack and which regularly visits all five sites. Subsequent enquiries confirm this to be Peter's new number and he is traced and arrested.

3. Officers request historic ICRs for his old mobile phone. Analysis shows consistent and repeated daily access to five websites;
www.chelseafotball.co.uk;
www.antiqueweapons.com;
www.americancars.com;
www.countrynwestern.com;
www.cowboyboots.com.

Robbery - ICR Purpose 'D' - Which internet service(s) have been used ?

1. Police are investigating the theft of an iPhone 6 belonging to a parliamentary aide.

Security fears exist over the fact that the phone contains personal contacts for a number of VIPs incl. government officials / celebrities.

The phone was stolen during a street robbery where the victim was forced to provide the PIN.

2. Traditional telephony enquiries indicate that the phone, although making no calls or texts, has had a new number installed and is being used on the internet.

Although currently switched off, it is known to be switched on sporadically, in the south east London area.

4. Historic ICRs for the new number identify repeated connections to a gaming site. Officers approach the gaming site against further legal notice and identify the relevant username and associated subscriber details. These resolve to an individual known to police. He is swiftly arrested in possession of the stolen phone.

3. In an effort to determine whether the internet usage provides any leads as to the identity of the suspect, officers could seek ICRs for the new number identified as being used in the stolen iPhone.

Serious Road Traffic Accident - ICR Purpose 'D' - Which internet service(s) have been used ?

1. A pedestrian is been hit by a car whilst crossing the road, suffering serious life changing injuries. The sole witness to the accident recalls, whilst giving their statement to police some time later, that the driver of the car was using his phone at the time of the accident, looking up too late to avoid the impact despite harsh braking.

2. Police seek independent evidence of the driver's alleged carelessness by making a telephony Communications Data request in respect of the drivers mobile phone. No traditional calls or texting is evident however.

4. These show connections to the eBay online auction site. Against further legal notice eBay confirm that a 'bid' was made at the time of the accident, in the last few seconds of an auction, from an account positively linked to the driver. Faced with this evidence, and that of the witness, the driver pleads guilty to driving without due care and attention.

3. In order to furnish the court with all available evidence, officers consider that the driver may have been using the internet at the time. Officers seek ICRs for the driver's mobile phone for a period covering a few minutes before the accident.

Child Sexual Exploitation (CSE) - ICR Purpose 'A' –
Which person or apparatus is using a specified internet service ?

1. Op Voicer

UK based paedophile ring (12 suspects) engaged in CSE on three victims aged below five, including one baby. Family groomed prior to birth.

Seven men convicted, including four teachers, and sentenced to a total of 107 years imprisonment.

2. Communications Data was used to;

- identify suspects;
- link them to each other;
- link them to abuse venue.

Suspects made extensive use of IP based communications, including 'live streaming' their abuse via a legitimate video conferencing facility hosted overseas.

4. Historic ICRs, would have identified UK subjects connected to the video conferencing facility at the time of the abuse.

This would include innocent parties using the facility – but would at least have given law enforcement further information to investigate.

3. One of the suspects was so appalled at the severity of the abuse that he came forward to police, providing details of the live streaming.

The video conferencing company was approached but had insufficient data to enable identification of all UK 'viewers.'

Cyber Bullying - ICR Purpose 'A' - Which person or apparatus is using a specified internet service ?

1. Head girl Jessica Lord (16) becomes depressed when someone using an email address in her name - jessicalord@yourmail.com) sends increasingly abusive and insulting emails to teachers and pupils at her school.

Eight emails are sent from the 'Yourmail' account, all within a two week period.

2. Hosted in Russia, the Yourmail App purports to offer anonymity to users by stripping customer IP addresses from the emails before transmission, making them untraceable through conventional means.

4. Those enquiries identify the same UK broadband account consistently accessing the Yourmail servers at approx. the same time as the emails were sent. Subscriber enquiries into the fixed broadband identify the home address of a sixth former at Jessica's school who subsequently admits the offence.

3. Officers ask UK CSPs to query ICRs for details of customers connecting to Yourmail at or immediately before the time the emails were sent. Officers further refine the query by seeking results only for connected customers within a 15 mile radius of Jessica's school.

Child Sexual Exploitation (CSE) – Grooming - ICR Purpose 'B' – Which Communication Service(s) have been used

1. Becky is 13 years old. She spends much of her free time on her phone on social media. One weekend she goes missing from home. Her parents try ringing her mobile but it is switched off. They contact her friends who eventually disclose that Becky recently met an '18-yr old boy called Wayne' on line, and had become infatuated with him.

2. A friend has seen his social media profile, believed from Facebook, and described him as good looking. They could not remember any other details about his profile but stated that Becky spent most of her time Instant Messaging (IM) him, although which App. she was using for this was not known. Her parents inform Police.

4. ICRs indicate recent use of the IM App RightNow. Enquiries with RightNow identify that Becky has been messaging mobile number 07992 334619, subsequently linked to a 40 year old subject on the National Sex Offenders Register - Donald Smith. Officers find Becky unharmed at his known address where she has been held against her will.

3. Missing person enquiries, including traditional telephony, prove ineffective in tracing Becky. In order to determine how, and with whom, Becky has been communicating online, officer expand their CD investigation to include historic ICRs for Becky's phone.

Possession of Terrorist Material - ICR Purpose 'C' – Which Illegal sites ?

1. John, in an effort to promote terrorist activity, creates a website containing pro-terrorist literature including documents about making improvised explosive devices and weapons, credit card fraud, secure communications and also displaying uncensored videos of successful terrorist attacks around the world together with supportive rhetoric.

2. Hosted in the Philippines, John provided false details to the hosting company, paying via Western Union. He administers the site from a laptop in the flat where he lives with his mother. Police receive an anonymous tip off about the site with John named as a possible administrator. Routine enquiries however do not uncover any obvious links to terrorism.

4. In order to support or negate a search warrant, officers seek ICRs for the home broadband. These show accesses to the site with analysis of upload rates matching recorded changes to the content of the site. Officers are able to obtain a warrant to search the address and seize the laptop. Forensic analysis identifies further evidence to charge.

3. Forensic recovery of the content of the site does confirm that the material falls within Sec. 58(1)(b) Terrorism Act 2000 as being of a kind likely to be useful to someone committing or preparing acts of terrorism.