ASSOCIATION OF
CHIEF POLICE OFFICERS

ACPO Data Communications Group

Single Point of Contact Data Survey

Between 4th June – 17th June 2012

SPoC Data Survey Results – 2012

Introduction and Background

This survey looks at the acquisition of communications data and provides the reader with an insight into the usage of such data across UK law enforcement. The survey results provide a very short snapshot of how communications data is used across law enforcement agencies. This data only relates to the acquisition of communications data under Chapter1 Part2 Regulation of Investigatory Powers Act 2000.

This survey was undertaken by 63 UK law enforcement agencies.

The survey took place between the 4th June and 17th June 2012 and requested details to be recorded that covered the following categories:

- Crime type under which the communications data was being requested
- Type of communications data being sought
- Age of communications data
- Grading of data requests
- Data subject identification
- Request identifier types

This survey was undertaken at the point when an application is submitted by the applicant to a SPoC. A SPoC is the Single Point of Contact who is an accredited individual responsible for acquiring the data from communication service provider.

This report will only provide the reader with percentages in relation to the acquisition of communications data. No numbers will be provided due to the interests of national security. ACPO Data Communication Group also provided a commitment to all those who took part in the survey to the fact that the actual numbers relating to the survey will not be published.

Full list of offences listed in descending order

Offences	Percentage
Drug Trafficking	17.7%
Drugs Misc	6.9%
Homicide (Any)	6.7%
Burglary (Res & Non Res)	6.5%
Fraud	6.5%
Missing / vulnerable persons	5.7%
Firearms	5.2%
Other	4.3%
Harassment & Stalking	3.4%
Malicious Comms	3.2%
Theft	3.0%
Serious Assault	2.9%
Child Abuse	2.9%
Other sexual	2.7%
Armed Robbery	2.7%
Rape	2.4%
Street Robbery	1.6%
Robbery	1.4%
Attempt Murder	1.1%
HMRC Offences	1.1%
Kidnap	1.1%
Terrorism	1.1%
Theft of/from MV	0.8%
Money Laundering	0.7%
Bribery &Corruption	0.7%
Blackmail	0.5%
People Trafficking	0.5%
999	0.5%
E-Crime	0.5%
Immigration	0.4%
Criminal Damage	0.4%
Bail & Courts	0.4%
Conspiracy	0.4%
Agg Burglary	0.4%
Arson	0.3%
Forgery Counterfeit	0.3%
Minor Assault	0.3%
Sexual offences	0.3%
Racial Hatred	0.3%
Threats to kill	0.3%
Gang related	0.3%
Public Order	0.3%
Sexual Other	0.2%
Bomb Hoax	0.1%
Obscene Pubs	0.1%
Sex Industry	0.1%
False Impt	0.1%
Vehicle crime	0.1%
Death by dangerous/careless	0.1%
Domestic abuse	0.1%
Explosives	0.1%
Witness intimidation	0.1%

Chart 1:

Chart 1 shows percentages in relation to the crime type that a communications data request was made during the survey period.

The following charts provide further information in relation to specific areas Crime Types, Time Periods (Age of Data) RIPA Request Types, Data Subjects and National Request Prioritisation Grades:

Crime Type

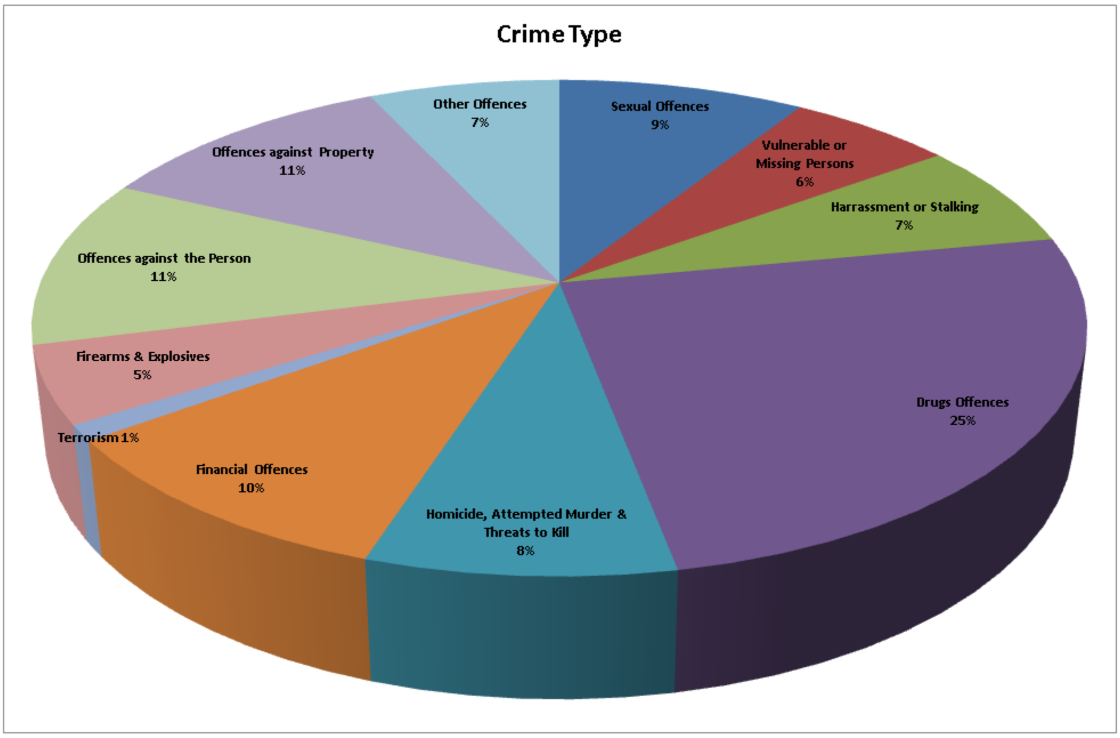

Chart 2: Breakdown of Enquiries by Crime Type

The above chart shows the relative proportions of different crime types for which communications data was requested.

- 25% of communications data requests related to drugs investigations.
- 9% of communications data requests related to sexual offences investigations.
- 6% of communications data requests related to missing/vulnerable persons investigations.
- 8% of communications data requests related to homicide, attempt murder and threats to kill investigations.
- 11% of communications data requests related to property offences, burglary and theft investigations.
- 7% of communications data requests related to harassment and stalking investigations.
- 5% of communications data requests related to firearms and explosives investigations.
- 10% of communications data requests related to financial offences, fraud and money laundering investigations.
- 11% of communications data requests related to offences against the person, robbery, assault, kidnap investigations.
- 7% of other communications data requests related to gangs, arson, bomb hoax and immigration investigations.
- 1% of communication data requests related to terrorism investigations.

Time Periods

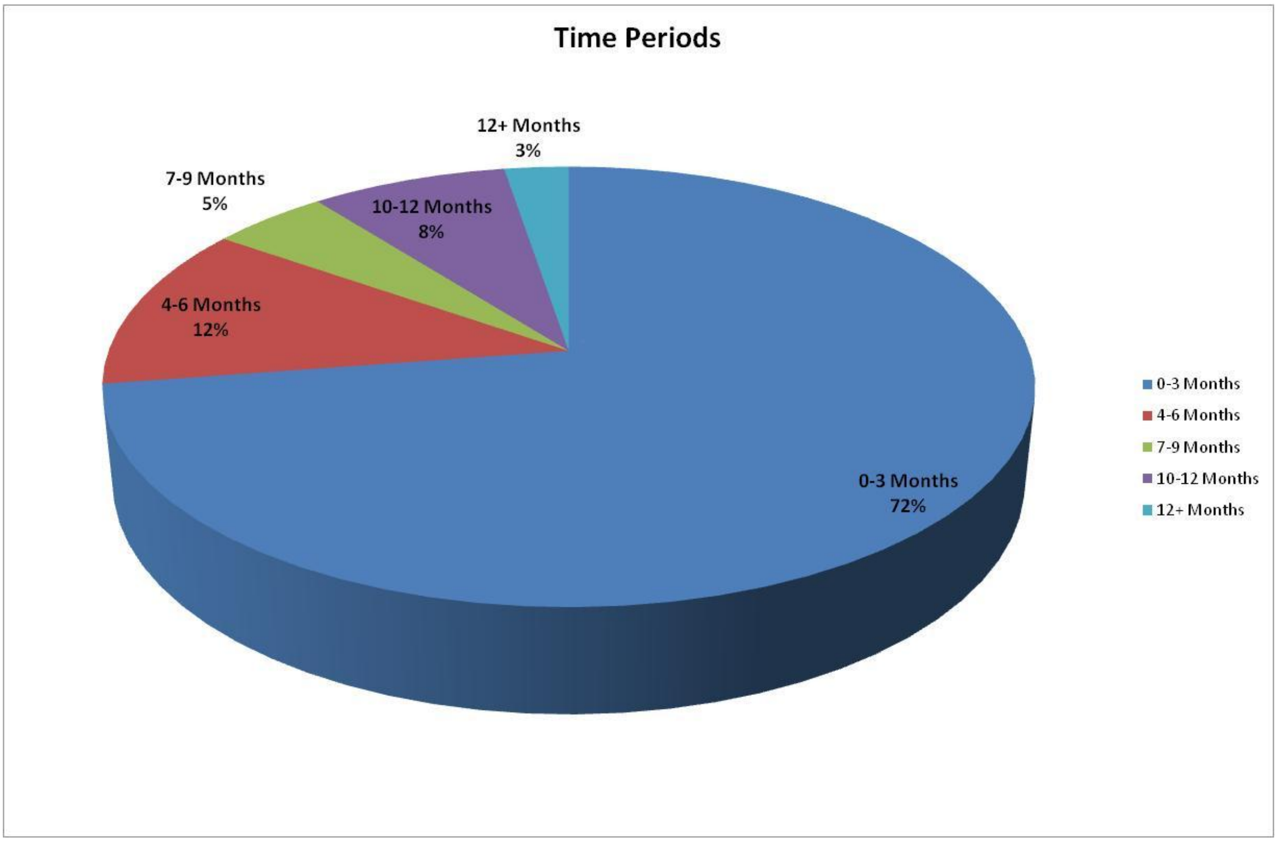

Chart 3: Breakdown of all Enquiries by Time Period

The above chart shows how long communication service providers have held the relevant data that was requested during the survey.

84% of communications data requested was up to 6 months old.

13% of communications data requested was 7 – 12 months old. What should be recognised is that 10-12 months data accounts for 8% this is higher than the 7-9 months data request as investigators realise that they risk losing this data as under the EUDRD, CSPs are not obliged to retain data beyond 12 months.

3% of communications data was more than 12 months old. Although this data does not need to be retained under the EUDRD, this data is retained by some communication service providers for their own business purposes.

RIPA Request Types

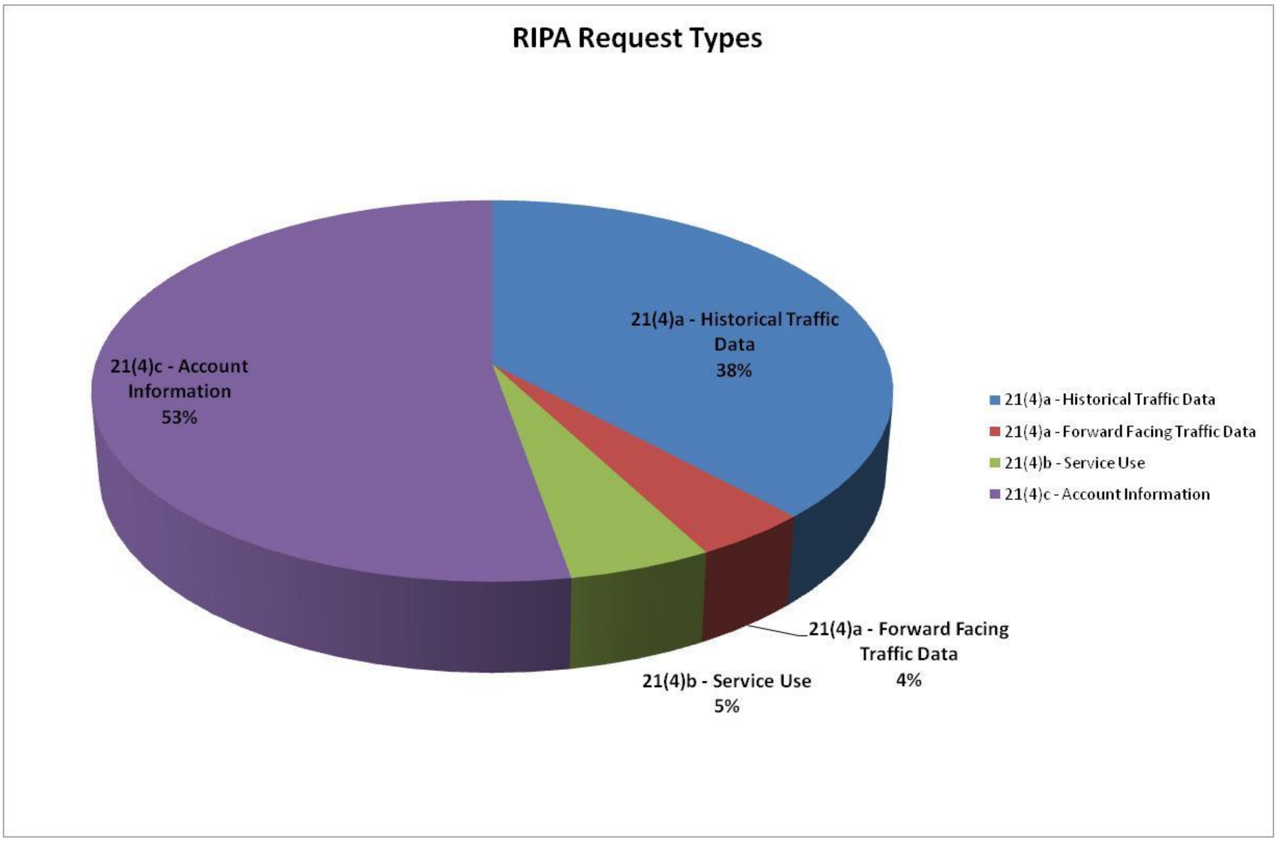

Chart 4: Breakdown of all enquiries by Request Type

Section 24 (1) of RIPA, in this Chapter “communications data” means any of the following:

(a)any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(Historic data requests relate to a date period in the past, whilst Forward Facing data requests relate to dates in the future)

(b) Any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c)any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

Data Subjects

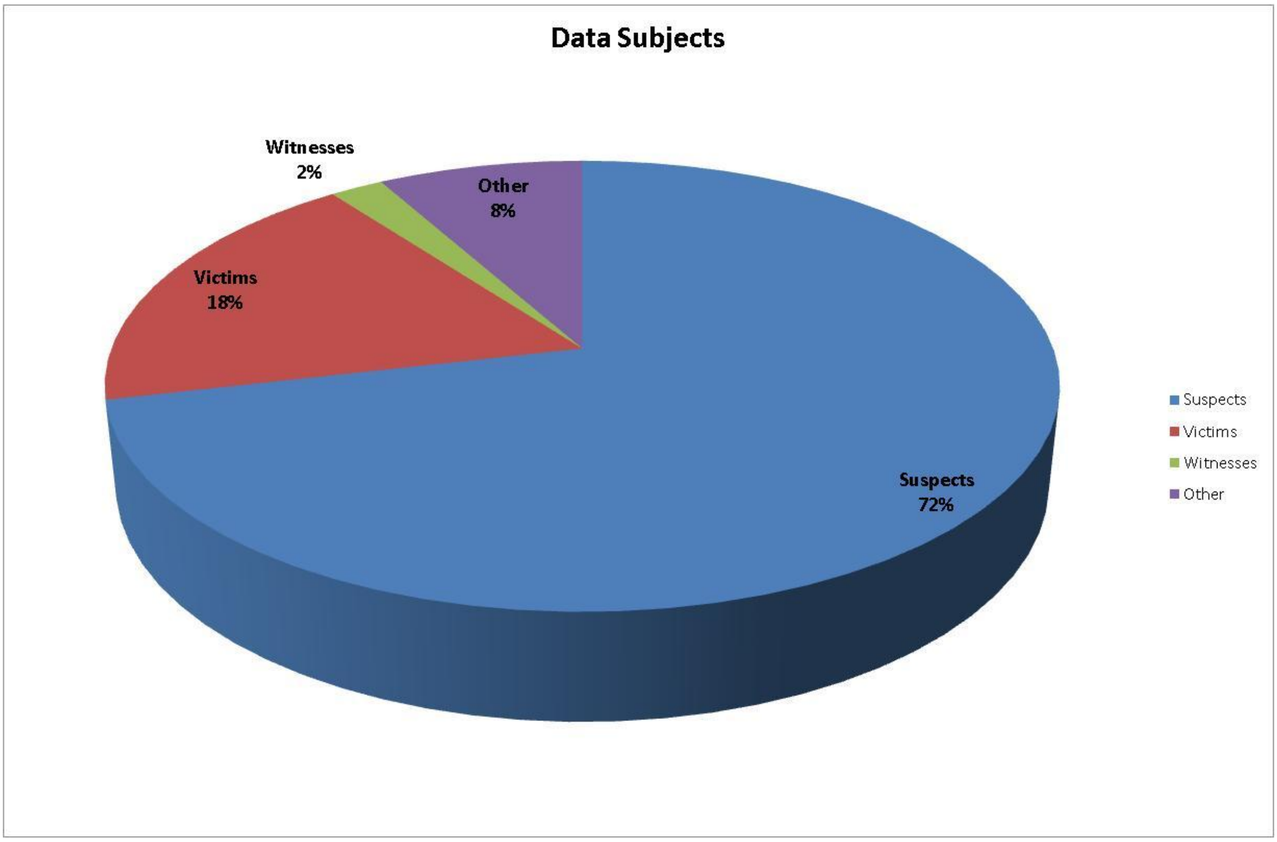

Chart 5: Breakdown of all enquiries by Data Subject types

The above chart identifies the person who the communications data request related to.

72% of the communications data requests related to suspect enquiries; this would clearly be in relation to the prevention and detection of crime. (A suspect is a person who has been arrested charged or believe to be responsible for a criminal offence at a particular time)

18% of the communications data requests related to victims of crime, this could be because their electronic device had been stolen or that communication data was used during the commission of a crime.

2% of the communications data requests related to witnesses, this could be identifying the actual time of a call, identification of a witness through possession of their telephone number.

8% of the communications data requests related to other which could relate to missing persons and vulnerable individuals, persons of interest during a homicide investigation or persons whose status at the time of the submission were unknown.

Whilst this report captures the number of data subjects listed within each application, it is important to remember that multiple applications are often submitted for a single investigation. In this survey 44 investigations accounted for 10 or more RIPA requests. There was one investigation in which over 40 RIPA requests were made.

Grades

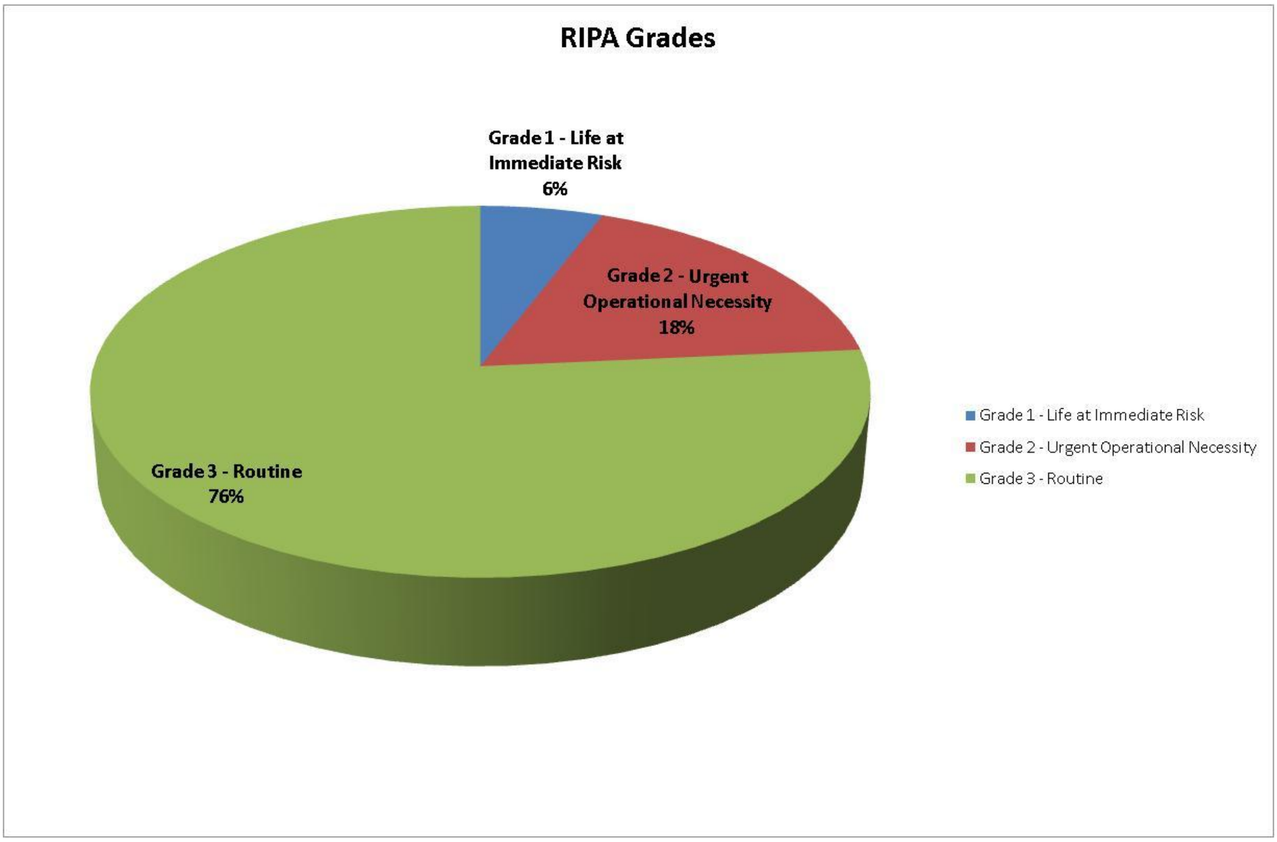

Chart 6: Breakdown of all enquiries by RIPA Grade

The above chart sets out the grade of the communications data request made by law enforcement to the communication service provider.

The Data Communications Group (DCG) which comprises representatives of CSPs, UK law enforcement and other public authorities to manage the strategic relationship between public authorities and the communications industry has adopted a grading scheme to indicate the appropriate timeliness of the response to requirements for disclosure of communications data. There are three grades:

- Grade 1 – an immediate threat to life;

- Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security;

- Grade 3 – other enquiries that are less time critical but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime

The emphasis within Grade 1 and 2 is the urgent provision of the communications data will have an immediate and positive impact on the investigation or operation

Significant Findings

What was evident from the survey is the fact that law enforcement is not able to define serious crime. Most definitions that are used are very subjective and what may be classed as serious to one victim may not be serious to another. (This is discussed further at Annex E)

The same can be said in relation to other less serious crimes, it is for this reason that we have not included percentages around these areas.

Crime Types

- 25% Drugs Investigations
- 7% Homicide Investigations
- 6% Missing Person and Vulnerable Person Investigations
- 21% Theft Act and Offences Against the Person Investigations

Data requested from communication service providers

- 95% Related to account information or traffic data
- 72% Requests were suspect related
- 20% Requests were victim or witness related
- 24% Requests were due to life at risk or urgent operational necessity

Older data is clearly used less, but data older than 6 months still accounts for a significant number of requests.

- 37% Of data requests relating to sexual offences was older than 6 months
- 27% Of data requests relating to Terrorism was older than 6 months
- 11% Of data requests relating to Drugs was older than 6 months
- 5% Of data requests relating to Homicide/Attempt Murder was older than 6 months
- 9% Of data requests relating to Firearms and Explosives was older than 6 months

Although this survey is only a snap shot over a two week period, this data does provide us with an insight into how, why and for what purpose communication data is used. Unfortunately some of the respondents may have misunderstood the required completion system and submitted data that needed normalisation before being used within this survey (The logic behind this normalisation is available if required).

It is clear that communications data is paramount in enabling law enforcement agencies to protect the vulnerable and saves lives.

Whatever steps criminals take to prevent their apprehension, they inevitably need to communicate with each other, use communication to commit the offence or have communication equipment with them when committing an offence. The increase in communication over the past decade and the increase predicted for the future make it even more important for law enforcement to be able to use the least intrusive investigative technique to prevent and detect crime today and in the future.

The acquisition of communications data is one of the least intrusive investigative techniques undertaken by law enforcement and is a process that is strictly managed and authorised by senior police officers in accordance with RIPA Chapter 1 Part 2.

The process ensures that the designated person complies with the requirements as set out in Chapter 1 Part 2 RIPA giving due consideration to peoples Human Rights, the necessity of the request, it must be for the protection of vulnerable persons or for the purpose of preventing or detecting crime, the authorising officer must be satisfied that it is necessary to use communications data in the investigation.

The proportionality, consideration will be given to balancing the seriousness of the crime being investigated and the interference with the privacy of the individual concerned.

The internal processes implemented and the national governance and inspection regime by IOCCO ensures that this investigative technique is only used in the protection of vulnerable persons and the prevention and detection of crime.

The need for law enforcement to maintain and improve on this capability is fundamental in our ability to keep pace with new technology, protect the vulnerable and continue to prevent and detect crime.