Home Office

Eniola Awoyale
Ofcom
Riverside House
2A Southwark Bridge Road
London
SE1 9HA

Dear Eniola,

Response Commercial Multi-User Gateway Review on behalf of the Investigatory Powers Unit (Home Office)

I am writing from the Investigatory Powers Unit in the Home Office to set out our concerns in relation to the use of commercial Multi User Gateways ('COMUGs'). I do not have any evidence, which would be pertinent to question 1, 2 or 3 of the consultation. The points raised below are in response to questions 4, 5 and 6 of the consultation.

When a caller dials a number, either from a fixed line or a mobile phone, information identifying the telephone number of the calling party is transmitted over the network. In the case of a mobile phone, location data is also transmitted. Such information is extensively used by law enforcement or emergency services for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health.

When a call is routed through a COMUG or a GSM Gateway, the originating caller's telephone number and location are not forwarded by the GSM gateway and, instead, are replaced by the number and location of the SIM card in the GSM gateway through which the call is routed. This means that the use of a COMUG or GSM gateway would make it almost impossible for the communications data of a call and caller to be ascertained.

In the event of an emergency where, for whatever reason, it has not been possible to ascertain where an individual is located, the inability to access communications data could prevent emergency services from being able to get to a person who is at serious risk of injury or death.

I thought it would be helpful to set out a couple of practical examples in which the use of COMUGs or GSM gateways could endanger the safety of life.

Communications data will often be vital in helping the National Crime Agency and other law enforcement agencies to track individuals, for example in a kidnapping case. If it were not possible to access data such as location data, then it would significantly impact their ability to locate either the victim or the person responsible for carrying out the crime.

Similarly, communications data plays a significant role for investigations into child sexual exploitation. For example call data enables law enforcement to build a pattern of abuse and often identifies previously unknown offenders and victims. Many high profile grooming cases, including those in Rochdale and Oxford, relied on communications data evidence to secure convictions.

Other public bodies also use communications data to prevent loss of life. For example the Maritime and Coastguard Agency will use location data to identify and locate vessels, which are lost at sea.

The use of GSM gateways in such scenarios could significantly interfere with law enforcement and public bodies' ability to use vital information linked to communications to prevent death or injury or damage to a person's physical or mental health. The Interception of Communications Commissioner's report covering 2015 states that 761,702 items of communications data were acquired by public authorities for various reasons, including to prevent death or preserve life.

Question 5 of the consultation asks whether any of the isues referred to in question 4 could be adequately addressed through a qualified exemption. If COMUGs or GSM gateways could be operated in such a way that it would not prevent or slow down access to communications data (including location data), which would allow law enforcement and public authorities to continue to use the information to prevent death or injury, then this may reduce the concern that the devices would endanger safety of life. However, based on our understanding of the way these devices operate, I do not believe that such conditions would be possible.

Yours sincerely,

Investigatory Powers Unit

Home Office