Australian Journal of Forensic Sciences, Volume 55, Issue 4, August 2022, pp. 560-571
DOI:10.1080/00450618.2022.2048691

When is a line of inquiry 'reasonable'? - a focus on digital devices

Graeme Horsman

Abstract

Many of the inquiries now made by law enforcement into suspected criminal conduct involve the interrogation of digital data generated by those parties subject to an investigation. This data often exists in large quantities where inquiry-irrelevant information is likely to be in abundance. When conducting an investigation that contains digital device/data, an investigatory team in England and Wales is under an obligation to pursue all reasonable lines of inquiry, however, determining 'reasonableness' is not straightforward where unfettered access to all available data should not be a default position in all cases and a suspect's right to privacy respected. This work examines when a line of inquiry is 'reasonable' if it involves a digital device, with the 'reasonable line of inquiry framework' offered to support investigatory teams to determine this. This approach is designed to support the production of transparent, robust and defensible decisions regarding the assessment of reasonableness.

Keywords: Forensic Science; Digital Forensics; Evidence; Reasonable Line of Inquiry; Digital Investigation

Introduction

Given the prevalence of digital device usage in society and the subsequent large volumes of complex data generated as a product of this, most individuals now maintain a substantial digital footprint that documents many of their daily activities. Whilst this information is often of value to law enforcement when conducting their inquiries, there is also the challenge of ensuring that any individual who is subject to an investigation has their right to privacy respected given the potential invasiveness of a digital investigation [1, 2]. As part of all investigations that involve a

digital device, any investigatory team is faced with a number of options in regards to progressing an inquiry. This includes decisions as to whether a device(s) may be of interest, whether it should be seized, whether to acquire its content and how (taking into account the various device acquisition methods available [3, 4]), and what should be analysed and why - the '*digital evidence strategy*'. When addressing all of these points, it must be emphasised that the job of an investigator is to explore all reasonable lines of inquiry [5], however, determining reasonableness may not always be straightforward, where unreasonable investigatory conduct may be deemed unlawful.

This work explores the concept of a digital 'reasonable line of inquiry' (RLOI) - one which concerns any digital device/data that is subject to investigation, where existing narratives surrounding this topic are highlighted in Section 2. The process of determining a RLOI is examined wherein Section 3 the 'RLOI framework' is offered, a method for supporting practitioners to determine the reasonableness of any proposed inquiry prior to its deployment. Finally, conclusions are drawn in Section 4.

2 Existing narrative on 'reasonable lines of inquiry'

Many jurisdictions worldwide will establish the legality of their law enforcement's investigative conduct through an evaluation of its reasonableness given the circumstances of any inquiry being conducted. This is an important process for the protection of both those subject to investigation, and those conducting an investigation to ensure their actions are not unlawful. Despite this, there is limited published guidance which discusses the concept of a reasonable lines of inquiry in relation to digital devices attributable to any legal system. Using available information, this work will utilise the position and available information in England and Wales as an example, where it is hoped many concepts will be applicable further afield.

In policing in England and Wales, the requirement for investigators to explore all RLOIs exists in all circumstances, however, this work will focus on RLOIs concerning digital device/data interrogation. Whilst an individual's personal and attributable digital data often being vast, when subject to a criminal inquiry it is likely neither proportionate nor necessary for law enforcement to interrogate it in its totality [6]. Doing so not only reduces the efficiency of the examination process due to the need to sift excess redundant information but also arguably increases the risk of error, misinterpretation and missing relevant content. Whilst these are quality assurance risks that must be managed by those conducting the work, there is a more fundamental issue. Those conducting an investigation are required to offset any potential line of inquiry against 'the need to respect the privacy of victims and witnesses while meeting disclosure obligations' [2]. In England and Wales, everyone has both the right to a fair trial under Article 6 of the European Convention of Human Rights and the right to private and family life under Article 8 [5] where this is acknowledged by the Attorney General's Office [5] -

> 'to comply with Article 6, during the course of an investigation, the investigator or prosecutor may decide that it is necessary to request and/or process personal or private information from a complainant or witness...when seeking to obtain and review such material, investigators and prosecutors should be aware that these lines of inquiry may engage that individual's Article 8 rights and those rights in respect of other parties within that material. Such material may also include sensitive data' [5] .

Further, a 'fair trial does not require consideration of irrelevant material. It does not require irrelevant material to be obtained or reviewed. It should not involve spurious applications or

arguments which aim to divert the trial process from examining the real issues before the court' [5]. When conducting an inquiry into a digital device, data should only be captured and/or analysed when it is lawful to do so, strictly necessary and proportionate where achieving this requires the practitioner to be acting in pursuance of a RLOI [5]. There is no definitive set of RLOIs, where an assessment of what is reasonable must be carried out on reasonableness must be carried out on a case-by-case basis [5, 7] and 'there is no 'one size fits all approach'' [8].

The Ministry of Justice [9] Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice' at 3.5 states that

> 'In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances. It is a matter for the investigator, with the assistance of the prosecutor if required, to decide what constitutes a reasonable line of inquiry in each case.' [9]

It is the role of the investigator to pursue all RLOIs, supported by the officer in charge of any investigation [9]. Of utmost importance is the requirement to pursue lines of inquiry that could be either exculpatory or inculpatory, where a failure to do so is a breach of duty as noted in *R v E 2018 EWCA 2426 (Crim)*. In relation to the content of any given digital device, an investigator may have to determine what may be of relevance to the inquiry given the known circumstances of it [8, 10], where seeking support from the officer in charge of the investigation is advised [11]. For example, in many cases and particularly where a mobile device is involved, it may be reasonable to secure access to and interrogate communication and/or social media data [12]. Following *Bater-James & Mohammed v R [2020] EWCA Crim 790*, a RLOI is not a speculative

one. It is also important to note that ‘reasonableness’ concerns those actions which are for both access to data and, any techniques deployed for the processing of it.

It is crucial that those forming part of any investigatory team are able to determine justifiable RLOIs consistently if they are to operate lawfully, however, this task is far from simple given the discretion available to investigators, the complexity of digital data and lack of foresight into the content stored on any devices. As a result, any determination of reasonableness may vary between investigators. In an effort to support this process, it is argued that the provision of a formalised structure for assessing whether any potential line of inquiry is reasonable would be beneficial. For that reason, the ‘RLOI framework’ is offered.

3 A structured approach

The process of determining whether any given line of inquiry is reasonable is complex and multifaceted given the unlimited number of circumstances that can manifest when digital devices and their data are involved in any alleged incident. The individual circumstances of every case must be evaluated as part of the identification of any RLOI, meaning that it is unlikely that a specific set of acceptable default RLOIs can ever be produced for use in all instances. Similarly, it is difficult to construct a set of definitive RLOIs to be applied even at an offence-level, as whilst some offences may maintain more obvious sources of relevant data and therefore related investigatory actions that are likely justifiable (consider investigations into indecent images of children, where a primary focus is to first establish the presence of any material of this type), others require less apparent forms of exploration in order to establish the extent of any alleged activities. Given these challenges, it is likely impossible that any formal guidance can provide an investigatory team with a set of defined RLOIs to be followed from the outset of an inquiry. As a result, it is suggested that focus should be placed upon the

decision-making process that is deployed as part of identifying a RLOI. This should not be an informal, *ad hoc* and solely 'hunch-based' process as approaching this task in such a way will arguably lead to the deployment of inconsistent or unsuitable investigative strategies that may impact the quality of any case outcome.

Formalising the process of determining the reasonableness of any line of inquiry is suggested as a way to increase both the accuracy of any final decision, whilst also demonstrating a robust, transparent and justifiable set of underpinning steps that led to the identification of a RLOI, a requirement acknowledged by the Attorney General's Office [5]. To achieve this, the 'RLOI framework' is offered.

3.1 The 'RLOI framework'

The RLOI framework (see Figure 1), referred to from hereon as 'the framework', provides nine stages that an investigatory team should engage with as part of determining whether any potential line of inquiry which they may want to follow, is reasonable, therefore ensuring that investigatory conduct is lawful. The framework only concerns only RLOIs in regards to digital devices/data. Any investigatory team may identify a number of lines of inquiry as part of their investigatory conduct where only those which are reasonable should be acted upon. The proposed framework provides nine stages that an investigatory team must address in relation to their line of inquiry and only once all nine are passed can a line of inquiry be considered reasonable. Each of these nine stages are discussed below.

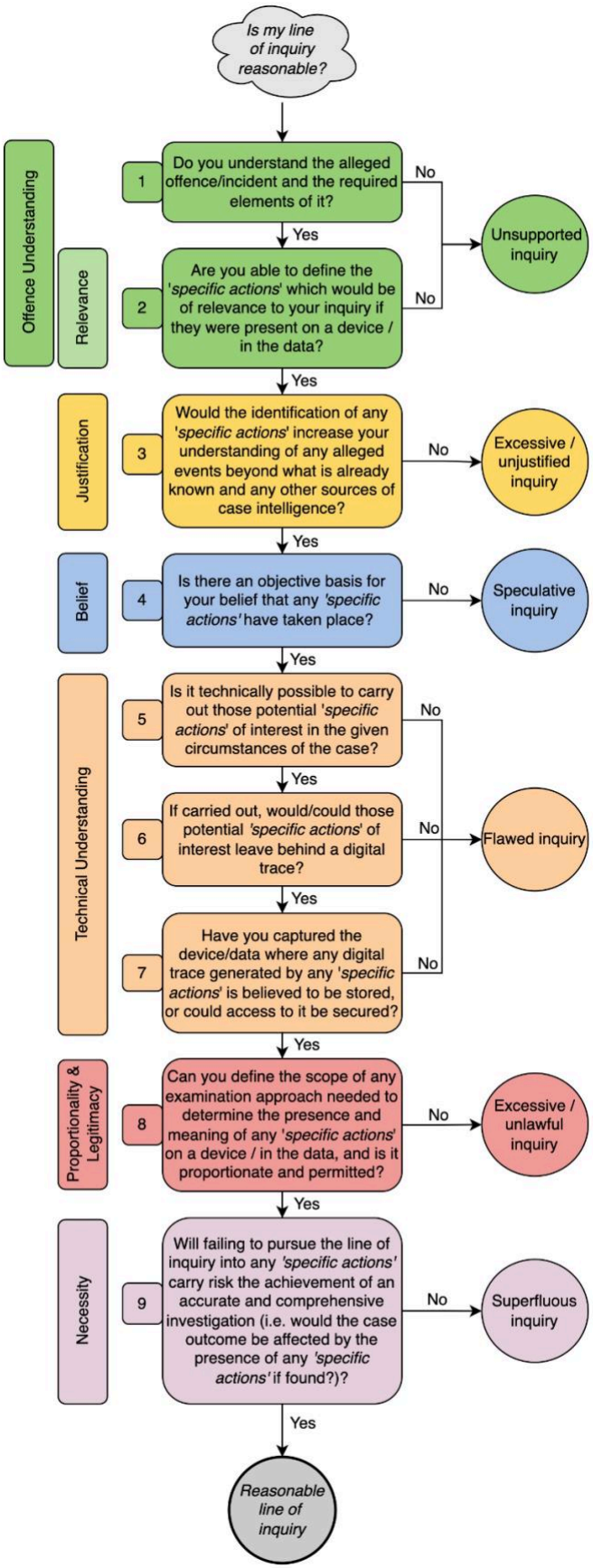

Figure 1: A reasonable line of inquiry framework.

3.1.1 Offence Understanding & Relevance

Stages one and two of the framework are in place to assess any investigative team's understanding of the suspected offence/incident and the relevance of any actions they may seek to inquire into, in regards to it [13]. Only once an investigatory team understand the suspected offence/incident can they begin to formulate a RLOI. For any digital data to be relevant to an inquiry, as defined by the Attorney General's Office [5] it must appear 'to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case'. Here, there are two stages an investigatory team must address:-

Stage 1 - 'Do you understand the alleged offence/incident and the required elements for it to be carried out?': Stage 1 requires the investigatory team to understand the elements and conduct associated with any alleged offence/incident as defined in law where this may require additional support for the interpretation of any offence guidelines. A RLOI cannot be formed if any suspected offence triggering an investigation is not understood.

Stage 2 - *'Are you able to define the 'specific actions' which would be of relevance to your inquiry if they were present on a device / in the data?'*: For any line of inquiry to be reasonable, it must concern conduct that is relevant to the inquiry. Whilst stage 1 requires a fundamental legal understanding of any alleged offence/incident, at Stage 2 an investigatory team must translate this understanding into the identification of relevant 'actions' which would be pertinent to their inquiry

if they were to be found on any device or data set [5]. In essence, digital conduct pertinent to an offence must be identifiable before it can be inquired into.

Any investigatory team that does not understand the alleged offence/incident or the types of conduct that may be associated with it cannot form a RLOI - this is fundamental to the process. Instead, any line of inquiry can only be classified as 'unsupported' wherein operational reality it is hoped that no inquiries are ever conducted before any alleged offence/incident is fully understood.

3.1.2 Justification

The College of Policing [7] that whatever 'an investigator considers reasonable or relevant may need to be justified later. It is, therefore, essential that they record their decisions and supporting rationale'. Once the investigatory team is considered to understand the offence, at Stage 3, they must determine whether there is justification for seeking to establish the presence of and/or access those actions which they have identified at Stage 2.

Stage 3 - '*Would the identification of any 'specific actions' increase your understanding of any alleged events beyond what is already known and any other sources of case intelligence?*': To be justifiable, the investigatory team must establish whether the identification of and/or access to any actions would offer insight/understanding of the alleged incident/offence which is above and beyond what is both already known and, what other sources of inquiry may offer, particularly if these other sources are less invasive. Where other sources of intelligence may offer a comparable understanding of the alleged incident/offence it may be necessary to establish which option may be preferable to pursue, taking

into account the needs of the investigation and the privacy-invasiveness of any process needed to access this content.

If any line of inquiry into digital actions would not provide an increased understanding of an incident/offence, then the line of inquiry can be considered excessive and unjustified.

3.1.3 Belief

Following Stage 4, an investigatory team must believe that any relevant actions/conduct have taken place, and there must be a reliable underpinning for such a belief as following *Bater-James & Mohammed v R [2020] EWCA Crim 790*, a RLOI cannot be speculative. As part of this process, investigators should also consider the prospect of obtaining relevant material [5].

> Stage 4 - '*Is there an objective basis for your belief that any 'specific actions' have taken place?*': Before an investigatory team can pursue a line of inquiry in search of specific conduct or actions, they must believe that such conduct or actions have taken place. This belief must be derived from reliable available information which is evidencable.

Any belief which has no objective foundation leads to an inquiry that is merely speculative.

3.1.4 Technical Understanding

A core part of the formation of a RLOI also involves understanding the technical underpinnings upon which any inquiry is to be based. This requires engagement with stages 5-7.

Stage 5 - *'Is it technically possible to carry out those potential 'specific actions' of interest in the given circumstances of the case?*': At Stage 5, an investigatory team must consider whether any actions they intend to inquire into are first technically possible to carry out. In some cases, this may be straightforward, for example, if an inquiry intends to establish whether there has been communication between parties using a specific mobile messaging platform. In this scenario, providing that any investigator can establish that the parties involved have the relevant equipment for doing these actions (an example may include determining that they have a mobile phone with a relevant contract or data connection) then these specific actions are clearly technically possible, meaning an inquiry into them has the potential to be reasonable. However, in some instances, determining the technical possibility of carrying out any alleged 'specific actions' of interest may be more difficult, where those conducting the investigation may not be familiar with the technology involved and misunderstand its capability and functionality. This is particularly a concern where an investigating team may lack the technical knowledge to accurately assess the viability of any alleged actions. It is recommended that where doubt exists with regards to assessing the technical possibility of a scenario, assistance should be sought to clarify the position from those who possess the knowledge to do so. Many law enforcement organisations deploy roles specifically for supporting investigating teams to deal with inquiries concerning digital devices, where examples include the role of the 'Digital Media Investigator' in England and Wales [15].

Stage 6 - '*If carried out, would/could those potential 'specific actions' of interest leave behind a digital trace?*': Whilst under Stage 5 any actions must be possible,

if they are, then an investigatory team must also consider whether such actions are likely to have left a digital trace behind on whatever system is the focus of an inquiry. Some digital actions may leave one or more traces on a system, for example, simple file accesses may create a series of operating system artefacts which show a file of interest has been interacted with by the system's user. However, some actions may leave limited system traces where examples may include the use of private browsing facilities [16]. Despite some actions being relevant to an inquiry, the absence of any trace to show that they have taken place would limit the value of the inquiry itself.

Stage 7 - '*Have you captured the device/data where any digital trace generated by any 'specific actions' is believed to be stored, or could access to it be secured?*': Finally, at Stage 7, the investigatory team should determine whether they have (or could practicably and lawfully obtain) access to the device/data where any digital traces of relevant actions are likely to be stored. Investigating teams should acknowledge that some traces may not be stored locally upon a seized device, where instead their presence made reside on server-side storage belonging to a service provider. In turn, where multiple devices exist or complex network structures are involved, the correct device(s) must be identified in order to prevent relevant content being missed during the seizure process, or unnecessary intrusion occurring through the seizure of irrelevant devices.

Any inquiry where a potential action of relevance is not technically possible, does not leave a trace or access to the trace itself cannot be acquired gives rise to a line of inquiry that is flawed.

3.1.5 Proportionality & Legitimacy

An investigatory team must also consider whether their potential line of inquiry is both legitimate and proportionate for it to be potentially reasonable.

> Stage 8 - '*Can you define the scope of any examination approach needed to determine the presence and meaning of any 'specific actions' on a device / in the data, and is it proportionate and permitted?*': An investigatory team must be able to define the scope of any examination procedures they intend to deploy/utilise as part of the examination of a device/data - 'a fair investigation does not mean an endless investigation' [5]. Examination procedures that provide unfettered access to device content/data should be avoided and substituted for more proportionate measures which align closely with the goal of the inquiry [18] [19]. In addition, any examination conduct must be lawfully permitted where the investigative team must consider the jurisdictional challenges and rules they are governed by. This includes consideration of the burden of proof defined in any legal system as well as the type of evidence they are expecting to acquire from the device they are seeking to investigate. In some cases, access to the content an investigating team may seek may be prohibited via mechanisms such as legal professional privilege, and the issues and risks this may pose to an inquiry should be identified and managed.

The deployment of an examination approach which cannot be defined in line with the needs of the inquiry and legal requirements leads to a line of inquiry that is both likely excessive and/or unlawful.

3.1.6 Necessity

At Stage 9, a potential line of inquiry must pass a test of necessity.

> Stage 9 - '*Will failing to pursue the line of inquiry into any 'specific actions' carry risk the achievement of an accurate and comprehensive investigation (i.e. would the case outcome be affected by the presence of any 'specific actions' if found?)?*': An investigatory team must consider how necessary it is for the line of inquiry into any alleged actions/conduct, taking into account the risk that not undertaking it poses to the accuracy and comprehensiveness of the investigation. In cases where the outcome may be materially impacted or the risk of harm being caused by failing to identify and examine any relevant actions is too great, then an inquiry may be considered necessary and these underpinning determinative factors should be evidenced as part of this process.

Any line of inquiry that is not necessary is a superfluous inquiry.

3.2 On completion

An investigatory team's line of inquiry is only reasonable if all nine stages of the framework can be passed. Approaching the assessment of reasonableness in this structured way provides any team with a transparent and evidenceable set of steps taken that have underpinned any decision to pursue a line of inquiry. Doing so acknowledges the comments of the Victims Commisioner [14] who suggests that any 'decision-making process of the authorised person in identifying a reasonable line of inquiry is recorded so that it can be scrutinised at a later date'.

4 The intention of the RLOI framework

There is arguably limited guidance available to support those conducting investigative work in relation to digital devices in order to determine whether their identified lines of inquiry are reasonable. Therefore, in reality, it is likely that any assessment of 'reasonableness' is likely to be conducted on an ad hoc and potentially inconsistent basis. The proposed RLOI is intended to offer formal support for this process and does not intend to 'lock in' the first responder to the approach stated, but to help provide some guidance and structure to the decision making process of determining 'reasonableness'. It is acknowledged that there may be some cases where deviation from this structure may occur but argued that in a lot of cases, the stages defined in the RLOI should be considered by the first responder when considering their course of actions.

It is also suggested that the RLOI promotes transparency in the investigative team's decision process or assessing the reasonableness of a line of inquiry as well as helping to ensure consistent decision making. Finally, the RLOI structure may support an assessment of accountability where it is suggested that those who deploy the RLOI make it easier for anyone evaluating this process to understand why they have reached the decision they have.

4.1 A practical example of the RLOI framework

In order to demonstrate the use of the RLOI framework proposed in this work, the following example is provided. Consider the scenario where a defendant is the subject of a relevant legal restraining order preventing them from making contact with a victim, and entering a defined area of where the victim is residing. Following reports from witnesses describing someone matching the description of the defendant in the vicinity of the victim's location, holding a

device up to the window of a dwelling believed to be that of the victim, the defendant has been arrested and found to be in possession of a smartphone device who states during interview that it is theirs. At this point, the officer in charge (OIC) of the investigation is in a position to consider whether it is reasonable to examine the smartphone as part of their inquiries in order to try and ascertain the defendant's conduct and location on the night of the alleged event. To support this decision-making process, the RLOI framework will be deployed.

Following Stages 1 & 2, the OIC must understand the remit of the regulations that the defendant is subject to, and the conduct required to breach them in order to ascertain whether an alleged breach of them could have taken place. If the defendant being in the location that is alleged by the witnesses would be considered 'breaching conduct', as the OIC proceeds with their inquiry, establishing the location of the defendant at the time of the alleged witness sighting becomes their focus.

Stage 3 requires the OIC to determine whether an examination of the mobile device is justified in order to support their investigation into the whereabouts of the defendant at the time of the alleged sighting, taking into account other potential sources of available intelligence. In this case, the only available sources of evidence are witness statements which may not definitively identify the defendant, at which point it could be argued that an examination of the defendant's phone may support the inquiry if there is information on it that can place the device at the time of the alleged breach (reasons why are discussed in later stages). Note, placing the device does not necessarily mean that the defendant is also present with it, but may be indicative following additional information.

At Stage 4 there must be an objective basis for believing that an examination of the defendant's smartphone may support the inquiry by revealing information about their location. Here, witness statements have provided an alleged sighting of the defendant holding a device in their hand and placing it at the window of the victim's dwelling. It is argued that there is a reasonable belief that this sighting could be of the device in possession of the defendant and that if the defendant was present at the time of the alledged sighting, then the device may also have been there as well.

At Stages 5, 6 & 7, the OIC must conduct a technical assessment of the smartphone and identify whether it is first possible for it to have recorded information that could disclose or indicate its location at the time of the alleged incident. Depending on the make and model of mobile devices, some services are known to maintain historical records of the device's location [17], and therefore it is technically possible for location history to be present on a device providing it is of the correct type. These traces can be stored on the device and by a service provider, and therefore appropriate access to the defendant's mobile device could could reveal this information.

Following Stage 8, the OIC should define the scope of the examination approach required to extract and identify this information and ensure that it is legal to undertake this investigatory work. If we assume that the device will be seized legally, then the OIC should consider what is required from the device itself where a discussion with relevantly trained staff may support the development of a digital evidence strategy. The OIC should consider the remit of accessing data and may opt to only extract content belonging to specific applications, log or operating system artefacts known to maintain relevant location data. Doing so ensures that the interrogation of the device is proportionate for the inquiry being conducted by maintaining

focus on information that would directly support the inquiry taking place (i.e. establishing the defendant's location).

Finally, Stage 9 considers the necessity of conducting the examination of the inquiry. If we consider here that the witness sightings may not be sufficient for determining the location of the defendant (in reality, many factors regarding their reliability must be evaluated by the OIC), then an interrogation of the device may be central to the success of the inquiry being conducted.

If the OIC completes the RLOI structure with positive responses to each stage then the inquiry into the smartphone's contents may be considered reasonable and defensible, with the process they have taken to reach this point evidenceable and transparent. However, in operational reality, an OIC should consider the potential for other factors to impact this process. For example, if CCTV exists which can formally ID the defendant at the time of the alleged breach then it may not be reasonable to examine the defendant's phone. Similarly, the OIC must determine whether the smartphone is an appropriate make and model for retaining location data and one that can be effectively examined by their forensic department.

5 Conclusion

The requirement to only follow those lines of inquiry that are reasonable presents a difficult challenge when considered in relation to digital devices and data. The vast amount both gathered and generated by individuals means that in any one case it is likely that data which is not relevant to an inquiry is likely to exist in far greater quantities than that which is important to understanding any potentially relevant conduct. Accessing and analysing this data should only be done when it is reasonable to do so, where the concept of reasonableness is likely difficult to define in all cases. The burden is placed upon any investigatory team to evidence

that any lines of inquiry pursued are reasonable, where this has already been noted here by the Attorney General's Office [5] to be a task that must be considered on a case by case basis. As a result, whilst it is not possible to propose a set of pre-defined RLOIs for use in all cases, supporting the 'reasonableness' decision-making process should be seen as beneficial. As a result, the RLOI framework has been proposed; a nine stage process of determining the reasonableness of a line of inquiry in relation to digital devices/data. Only once an investigatory team is able to address all nine stages can any line of inquiry which they are considering be deemed reasonable, and therefore proceedable. Failure at any stage of the framework indicates that a line of inquiry should not be pursued.

The framework not only offers a preventative measure against the deployment of non-reasonable lines of inquiry but also provides the clear and demonstrable set of criteria that has been used to underpin any decision made by the investigative team.

References

1. The Information Commissioner's Office (2020) 'Mobile phone data extraction by police forces in England and Wales' Available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf (Accessed: 26 October 2021)

2. National Police Chiefs' Council, (2021) 'Police update notice for permission to search for relevant information on digital devices' Available at: https://news.npcc.police.uk/releases/police-update-notice-for-permission-to-search-

for-relevant-information-orn-digital-devices (Accessed: 26 October 2021)

3. Sammons, J., 2012. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

4. Mikhaylov, I., 2017. Mobile Forensics Cookbook: Data acquisition, extraction, recovery techniques, and investigations using modern forensic tools. Packt Publishing Ltd.

5. Attorney General's Office (2020) 'Attorney General's Guidelines on Disclosure' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923774/Attorney_General_s_Guidelines_on_Disclosure_2020_NOT_YET_IN_FORCE.pdf (Accessed: 26 October 2021)

6. Anderson, P., Sampson, D. and Gilroy, S., 2021, September. Digital investigations: relevance and confidence in disclosure. In ERA Forum (pp. 1-13). Springer Berlin Heidelberg.

7. College of Policing, (2021) 'Investigation process' Available at: https://www.app.college.police.uk/app-content/investigations/investigation-process/#reasonable-and-relevant-enquiries.

8. Dorset Police (n.d.) 'WHAT HAPPENS NEXT?' Available at: https://www.dorset.police.uk/media/66532/investigation_timeline-dorset-master.pdf

(Accessed: 26 October 2021)

9. Ministry of Justice (2020) Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931173/Criminal-procedure-and-investigations-act-1996.pdf (Accessed: 26 October 2021)

10. Ministry of Justice (2015) Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf (Accessed: 26 October 2021)

11. Crown Office and Procurator Fiscal Service, (2014) 'Disclosure Manual' Available at: https://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Disclosur_Manual/Chapter%203.pdf (Accessed: 26 October 2021)

12. Crown Prosecution service (2018) 'Disclosure - A guide to "reasonable lines of inquiry" and communications evidence' Available at: https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence (Accessed: 26 October 2021)

13. Police Scotland (n.d.) 'DIGITAL DEVICE EXAMINATION – PRINCIPLES' Available at: https://www.scotland.police.uk/spa-media/ooadfwm4/digital-device-

examination.pdf

14. Victims Commisioner (2021) ‘Background on the impact of digital disclosure on victims’ Available at: https://bills.parliament.uk/publications/41921/documents/412 (Accessed: 26 October 2021)
15. College of Policing (2022) ‘Digital Media Investigator’ Available at: https://profdev.college.police.uk/professional-profile/digital-media-investigator/ (Accessed: 12 January 2022)
16. Horsman, G., 2020. The challenge of identifying historic ‘private browsing’ sessions on suspect devices. Forensic Science International: Digital Investigation, 34, p.300980.
17. Google, (2022) ‘Manage your Location History’ Available at: https://support.google.com/android/answer/3118687?hl=en-GB (Accessed: 12 January 2022)
18. ICO 2020. Mobile phone data Extraction by police forces in England and Wales. Available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf (Accessed: 8 December 2020)
19. ICO, 2021. ‘Guide to Law Enforcement Processing’ Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/ (Accessed: 28 August 2021)

When is a line of inquiry ‘reasonable’? - a focus on digital devices

Horsman, Graeme

2022-03-18

Horsman G. (2022) When is a line of inquiry ‘reasonable’? - a focus on digital devices. Australian Journal of Forensic Sciences, Volume 55, Issue 4, August 2022, pp. 560-571 https://doi.org/10.1080/00450618.2022.2048691