OFFICIAL REPORT
AITHISG OIFIGEIL

# Justice Sub-Committee on Policing

**Thursday 13 September 2018**

Session 5

The Scottish Parliament
Pàrlamaid na h-Alba

# Thursday 13 September 2018

## CONTENTS



## JUSTICE SUB-COMMITTEE ON POLICING
**9th Meeting 2018, Session 5**

**CONVENER**

*John Finnie (Highlands and Islands) (Green)

**DEPUTY CONVENER**

*Margaret Mitchell (Central Scotland) (Con)

**COMMITTEE MEMBERS**

*Daniel Johnson (Edinburgh Southern) (Lab)
*Fulton MacGregor (Coatbridge and Chryston) (SNP)
*Rona Mackay (Strathkelvin and Bearsden) (SNP)
*Liam McArthur (Orkney Islands) (LD)
*Stewart Stevenson (Banffshire and Buchan Coast) (SNP)

*attended

**THE FOLLOWING ALSO PARTICIPATED:**

Peter Benson (Police Scotland)
David Freeland (Information Commissioner's Office)
Detective Chief Superintendent Gerry McLean (Police Scotland)
Diego Quiroz (Scottish Human Rights Commission)

**CLERK TO THE COMMITTEE**

Diane Barr

**LOCATION**

The David Livingstone Room (CR6)

# Scottish Parliament

## Justice Sub-Committee on Policing

*Thursday 13 September 2018*

*[The Convener opened the meeting at 13:01]*

## Interests

**The Convener (John Finnie):** Feasgar math, a h-uile duine, agus fàilte. Good afternoon, everyone, and welcome to the Justice Sub-Committee on Policing. This is our ninth meeting in 2018. We have received no apologies. Before we begin, I place on record my thanks to Ben Macpherson for his work as a member of the sub-committee and wish him all the very best in his ministerial role.

I welcome Fulton MacGregor to the sub-committee and back to the Justice Committee, which is the parent committee. Are there any declarations of interest that you are required to make?

**Fulton MacGregor (Coatbridge and Chryston) (SNP):** Thanks, convener. I have no relevant declarations of interest for the sub-committee.

## Decision on Taking Business in Private

13:02

**The Convener:** The next item is a decision on taking business in private. Under item 4, we will consider our approach to the pre-budget scrutiny of the Scottish Government's draft budget 2019-20. Are members agreed to take that item in private?

**Members** *indicated agreement.*

## Digital Device Triage Systems

13:02

**The Convener:** The next item is on Police Scotland's proposed use of digital device triage systems. We will take evidence from David Freeland, a senior policy officer at the Information Commissioner's Office; Detective Chief Superintendent Gerry McLean, the head of organised crime and counter-terrorism at Police Scotland; Peter Benson, the cybercrime forensic team leader at Police Scotland; and Diego Quiroz, a policy officer at the Scottish Human Rights Commission. You are all very welcome. I thank those of you who have given us written submissions—that is always very helpful.

I will kick off with some questions for Chief Superintendent McLean. Thank you for the various documents that have been sent to the committee. The trials commenced in 2016. Why, some two years later, is the data protection impact assessment still marked as a draft?

**Detective Chief Superintendent Gerry McLean (Police Scotland):** Thank you for inviting us along to give evidence today, convener. We welcome the opportunity to do so and, more particularly, to answer any questions that you put to us.

The finance framework for 2016 and 2017 did not support the trials at that time. We were keen to progress those internal trials, which were designed to look at the benefits realisation to front-line officers, service improvement and the experience of the public, but the constraints within the force at that time did not allow us to do so, so we took some advice. We obviously did not have the general data protection regulation at that time, so the impact assessments that were considered were different from where we are now.

We drafted the DPIA and the equality and human rights impact assessment after consultation with some of the reference groups, which we will perhaps speak about later. We see those documents very much as needing to be completed but, at the moment, they are living documents until everyone has had a chance to examine them and make a contribution on them. Even as recently as last week, some of the groups that have engaged through the external reference group were making contributions, particularly around the EHRIA. We hope to get those documents finally signed off and get some agreement across the various groups that have contributed to them.

**The Convener:** Is there any recognition on the part of Police Scotland that best practice would be to make an assessment in advance of doing

something rather than at the conclusion? I welcome where we are, and I welcome the engagement with the stakeholder and reference groups, which is very positive. However, it would be good to hear a recognition of that from Police Scotland.

**Detective Chief Superintendent McLean:** Yes, convener. I accept that we need to make some assessment of that. It is what I was talking about when I mentioned the benefits realisation and the impact on the wider public of introducing new technologies, so I totally accept the position that you have described. Conversely, it is only after we have thought about the introduction of the technology, the training implications, how it is going to be delivered, the audit compliance around that and the wider impact on the public that we can truly articulate those things within the various impact assessments. Nevertheless, I take your point.

**The Convener:** I accept that the DPIA is a developing document. If, as you say, the situation is evolving, has it changed much from what you would have originally assessed?

**Detective Chief Superintendent McLean:** There have been fairly minor changes. Some of the contributions in the external reference group were around the various articles of the European convention on human rights—particularly article 6, the right to a fair trial, and article 8, the right to privacy. Generally, the group would like to see a bit more detail and a fleshing out of some of the considerations in the document. There is perhaps a bit too much police jargon, and it needs to detail some of the wider implications for the general public. That is why we are quickly revising that document. We hope to get the document signed off in the next few weeks.

**Diego Quiroz (Scottish Human Rights Commission):** Thank you very much for inviting the commission along today.

This is a really good question to ask of the police—the convener asked the same question on 10 May. The human rights impact assessment and the equality impact assessment are essential prerequisites, as they ensure that policy, programmes and projects are compliant with human rights. They should be produced in advance, even if you are running a trial. The commission has significant concerns about the trial of 600 phones and the legality of how the process has been run so far.

We must also acknowledge that we do not have the full information about the trial—I just learned that earlier. Although Police Scotland has recently adopted an open and multistakeholder approach, that has not been the case from the outset. That highlights the wider issue of the importance of a human rights-based approach in policing—something that we have recommended for a while.

If you will allow me, I will focus on the current human rights impact assessment, which, I am afraid, highlights a number of concerns. First, the document conflates certain legislative protections with human rights protections. Because of the time constraints, I will focus on only one of those. The analysis of article 8 relies heavily on data protection requirements. It reads:

> "this article will be heavily protected due to the documents compliance with GDPR".

The data protection framework, which is about data processing, is separate from the human rights framework, and compliance with that framework, although necessary, is not sufficient by itself to meet human rights requirements. That is a crucial point, and it requires further analysis by the police. I do not think that only a bit of tweaking or analysis is needed; it requires much more further analysis because the distinction between privacy and data protection is fundamental to understanding how they interact and complement each other.

Privacy concerns arise when personally identifiable information is collected, stored and used—which is not the case here, although it is the case with hubs—and the legal question focuses on whether there is justified or unjustified interference. Data protection is about securing data against unauthorised access—it is a technical question about the conditions that are required to facilitate full and lawful protection of data. We are worried that those two distinct issues are being treated as the same and synonymous in the human rights impact assessment. Data protection is an expression of the right to privacy but does not address the same issue as is addressed under the ECHR.

There are other issues, which I can go back to if the committee wants.

**The Convener:** Thank you very much for that. We will pick up on those issues, and there is always the opportunity to write to us to clarify points.

Do you wish to respond to that briefly, Detective Chief Superintendent McLean?

**Detective Chief Superintendent McLean:** If I may, convener. I accept all the points that Diego Quiroz makes. I apologise to him, to the convener and to the committee if I was too general in my view of where we are with the revision work around the impact assessments. I readily accept the points that Diego Quiroz has made. They are the same points that Privacy International made at the most recent reference group meeting, and they are the substantive points that we are working on.

**The Convener:** Before I invite other members to ask questions, can you say where we are with progress? Are we on schedule for the start date that you anticipated? Will all these mechanisms be in place prior to that? I would like an assurance on that, please.

**Detective Chief Superintendent McLean:** I previously briefed the committee that we had an indicative roll-out date of around October 2018. However, we recognise the importance of the consultation. A lot of progress is being made on the training delivery. We are refining what that will look like across the whole force area to ensure that there is adequate coverage through local officers providing local delivery.

We have now had two meetings of the stakeholders group—the group involving organisations such as the Scottish Police Federation, Her Majesty's inspectorate of constabulary in Scotland and others who might be said to be more integral to the criminal justice system. The most recent of those meetings took place yesterday. We have also had two meetings of the external reference group, to which Open Rights Group, Privacy International, the Scottish Human Rights Commission, the Information Commissioner's Office and others are invited. The most recent meeting of that group was last week.

We are focused on the legal basis for the examination of devices and the processes around the use of cyberkiosks. In my view, we are less focused on the equipment itself, the substantive point being that the equipment does not extract or store data. It is the wider considerations that we are focused on, and Diego Quiroz has touched on some of them.

We are working on three documents. One is a public information leaflet; one is a principles-of-use document that articulates the mechanisms by which data will be managed and the cyberkiosks will be used; and one is an internal document for the users—a toolkit. We hope that, if we can get all those documents that we are currently working on ready by about the end of October, when those groups will meet again, we can look at a potential roll-out commencing in early November.

**The Convener:** Thank you. I said that that was my final question, but I have another question that follows on from one of your points. I am looking at the minute of the meeting of the reference group on 26 July. The issue was raised of a situation in which a witness hands over their phone and subsequently changes their mind. There is reference to discussions with the Crown Office and Procurator Fiscal Service about that. Has that issue been resolved? A lot of people would understand that a different arrangement would apply to a witness than would apply to a suspect or an accused.

**Detective Chief Superintendent McLean:** We discussed that issue at the stakeholders group. As I am sure the committee recognises, it is very difficult to get a policy that covers every eventuality, but we have been explicit about the legal basis on which the police would seize a phone, whether from a witness, from a victim or from an accused person. The legal basis is threefold. It would be under warrant; on some occasions, it would be under a statutory framework such as the Misuse of Drugs Act 1971; more frequently, it would be under a common-law power. Therefore, even in the eventuality that a witness offered a device, saying that there was something on it that had a material bearing on a matter under investigation, the legal basis on which the police would hold that device would be a common-law power.

It is difficult to cover every eventuality concerning what can be examined on a device, what can be offered and whether the witness can get their device back. It will depend on the case under investigation. Clearly, the police have some discretion at their disposal; however, as soon as the device has entered the evidential chain, it may well be a matter for the prosecution and, ultimately, the court to deem the fairness of the device having been taken and the material importance of the content on it.

**The Convener:** Yet the minute specifically says that the Crown Office and Procurator Fiscal Service's position is that that is an operational matter for the police.

**Detective Chief Superintendent McLean:** That is about the discretion element of it and the statutory obligations that we have under the disclosure legislation. The police have to apply a test of relevance: is the phone relevant to the matter under investigation, should it be taken and should it be examined? As I say, it is difficult to cover every eventuality.

**The Convener:** I understand that. Would it be possible for us to get a number of brief examples of the circumstances in which a phone has been seized from an accused person, a suspect or a witness? That would give the committee some understanding of the parameters and what principles applied. I appreciate that such seizures would have taken place under the trial.

**Detective Chief Superintendent McLean:** Would you like me to provide that evidence at a later stage?

**The Convener:** Yes, please. In writing. Thank you.

**Detective Chief Superintendent McLean:** I am happy to do so, convener.

**Margaret Mitchell (Central Scotland) (Con):** Good afternoon, gentlemen. Can you give further information on the rationale for the divisional breakdown of the cyberkiosk terminals and the factors that were taken into account in deciding where they would be located and the number of them that would be allocated? For example, why does Q division in Lanarkshire have four terminals and other divisions have only two?

**Detective Chief Superintendent McLean:** There has been a lot of close working between the cybercrime hubs, cybercrime professionals and the divisional management teams in each of the 13 local policing areas in Scotland. We provided demand analysis. We asked what all the devices that had been submitted in the past couple of years looked like pro rata per local policing area. We then worked with the local policing areas for them to decide how the approach could be resourced in their deployment model with the cadre of trained officers available and at their disposal and the demand that they thought they might see across their divisions. How many devices they could take or support in each of their areas was very much a matter for them, with the statistical data that we provided per division.

Members will see the situation in some of the larger geographic areas, particularly in the north of Scotland. A division will take five terminals and N division will take four. That is to do with the geographic challenges in those areas. The local policing areas in the central belt are different sizes and they have different crime levels, so they have different digital forensic needs. It was a matter of working very closely with the divisional management teams. The number and locations of the terminals were all set locally by the divisional management teams in the local policing areas.

**Margaret Mitchell:** Were they the ultimate arbiter of the number of terminals in each division? Was there any disagreement on or discussion about the number?

**Detective Chief Superintendent McLean:** As I understand it, it was all fairly amicable and there were no real issues. The question to ask is whether the figures are appropriate and whether they will change. There will be a continual review process. Once we roll out the kiosks, we will continue to review the demand, the number of submissions, the benefits in areas, and the demands in local policing. Can the cadre of trained officers continue to be resourced if there is a turnover of staff? The figures will be under continual review, and those figures may be adjusted in that journey.

13:15

**Rona Mackay (Strathkelvin and Bearsden) (SNP):** Good afternoon, gentlemen. Can you give us a timescale for the review process? Is there an end date for it, after which you will say that you will consider an expansion and rolling out more terminals? Is that the plan?

**Detective Chief Superintendent McLean:** It has come out loud and clear that audit and compliance are a really important part of data security and privacy. We propose an incremental roll-out to a full roll-out over perhaps three months once we go live. It will be simultaneous in the east, north and west of the country. Our aspiration is that that will be done by the early part of 2019.

On going live in a particular area, we will look to start to generate information and performance data on the number of submissions and any breaches and non-compliance issues. That information would be reported through the Scottish Police Authority. We are also looking at the publication scheme to see whether we can make that data publicly available on the Police Scotland website. Therefore, the approach is very much public facing.

Our aim is to review the deployment model probably after about six months. From the point of going live in one part of the country, it will probably take us around three months to complete coverage of the whole country. We will do a full review of the whole process probably in around six months, and we will capture learning as we move from one area to the next so that the product that is delivered towards the end of the roll-out will be the best that we can have.

**Rona Mackay:** If you found that the product was being underused or not used in a particular area, would it be taken away? Is that the idea?

**Detective Chief Superintendent McLean:** The approach might not be as extreme as that. I think that there would be an opportunity to do a bit of deconfliction. If some local policing areas had underused devices and some had greater demand, there would be a conversation to be had about that. We will approach the matter in a positive fashion, but recognise the public interest and our responsibilities. If we start to realise the benefits that we think we will realise, whether we would look at making greater use of that type of technology would probably be a consideration. We could consider whether the demand existed or whether we had quelled a lot of the demand and stripped a lot of the volume out at the front end.

**Diego Quiroz:** Before I talk about deployment, I would like to roll back a bit to the question about legality, which is very important under human rights and the rule of law. There are two aspects, one of which is the existence of a legal framework.

Some of that has been expressed by Police Scotland. Once there is a legal framework, the question is about its quality.

Accessing sensitive and personal data certainly engages article 8 of the European convention on human rights. A cluster of cases from the European Court of Human Rights in Strasbourg—everything from Copland v United Kingdom to Kennedy v United Kingdom and S and Marper v United Kingdom—confirms that. That is quite clear.

We know that cyberkiosks can access private data—everything from texts to photos and web browsing—and even more sensitive data, such as biometric data. My phone has my fingerprints and my voice, for example. In a criminal law context, there can even be information about journalistic material or legally privileged information. That is incredibly sensitive data, so the framework and its legality are important.

It is possible to find more private information in a mobile phone than in a bedroom or a house. Let us keep with that metaphor. The police need a warrant to search a house. That being the case, a more or equally intrusive digital measure will certainly require a similar safeguard. However, this is the first time that I have heard the police mentioning the idea of using warrants. I think that the Commission would not be satisfied if there was no similar legal safeguard to that which there is when a house is searched in Scotland.

**The Convener:** I took that to be one of the options that could be used. Chief Superintendent McLean, could you clarify the issue of the use of a warrant? After that, Mr Freeland might like to comment on what he has heard.

**Detective Chief Superintendent McLean:** As I said, the legal basis for seizure is threefold—it might involve the use of a warrant, the use of a statutory power that the police had at the time or the use of a common-law power. In relation to the use of a warrant, I meant that it empowers the police to search a particular location at a particular time to recover a number of items that are pertinent to the investigation. A warrant would empower the police to carry out a search, which might include the taking of mobile devices, but it has been a long-held principle in Scottish law, and it is the view of the Crown Office, as articulated through our stakeholder reference group, that once a warrant, a statutory power or a common-law power has been used, we are entitled to examine electronic digital devices.

**David Freeland (Information Commissioner's Office):** I would like to make the committee aware of the fact that the issue of the use of digital evidence and how it is obtained is a priority issue for our office at the moment. We are looking at it across the United Kingdom in relation to all law enforcement agencies. In doing so, we are supported by the information that Privacy International has already provided us with on the use of such evidence by police forces.

The legality of obtaining the data is an important area, which we want to do more work to understand, particularly in relation to the statutory powers. We want to find out whether those statutory powers are fit for purpose and whether they allow an intrusion into the digital space, given that they might have been formulated decades ago when the issue was not considered. We want to understand better what the legal position is. Is such action lawful in the first place? If it is not lawful in the first place, a legislative solution needs to be found to bring the statutory powers up to date.

**The Convener:** Who would determine that, Mr Freeland?

**David Freeland:** Ultimately, the legal basis is determined between the Parliament and the courts. We would need to make sure that there was a substantive legal basis, but the issue is one that I, along with Diego Quiroz and others, will want to explore further with Police Scotland.

**Daniel Johnson (Edinburgh Southern) (Lab):** If you do not mind me saying so, the statement that you have just made is quite a showstopper. You are saying that you are not clear whether there is a sufficient legal basis for the police to access the data in this way, using such devices. Is that a correct—

**David Freeland:** For our purposes, we need to know that the processing of personal data is lawful. The police have said what their various lawful bases are—they involve the use of a warrant or statutory or common-law powers. We just want to understand the extent of those powers. We are not experts in criminal law itself, so we need to do some work to understand whether such activity is lawful and fair.

**Daniel Johnson:** I would be interested to get a response from the police on that. Are you confident that you can access such data lawfully? Are there sufficient grounds to do so on the basis of existing legislation?

**Detective Chief Superintendent McLean:** To be quite explicit, I am confident of that, and I think that that is borne out by the many prosecutions that go through Scottish courts and are examined every day and every year. Whenever there have been any challenges around that, the court has upheld the position that the police have had the power to examine those devices. I have previously talked to this committee about the 15,000 or so devices that go through our cybercrime hubs every year and then make their way into the criminal

justice system. Any such challenges are pushed back.

That position is held by the Crown Office, too. In the stakeholders group, we have asked it whether it is comfortable with that position, and it would support that.

**Daniel Johnson:** I want to follow up on the point that Mr Quiroz raised. The sheer scope of the information that is now held on mobile phones is very significant, so there is an issue to do with having access to that and the hurdles and protections around that.

There is another point, which is associated but not identical. Permission may be granted to access one form of data for one purpose, but what protections and provisions exist to prevent the accessing of other kinds of data? Is that a valid concern? I would be very interested to hear from Mr Freeland on that, too.

**Diego Quiroz:** That is absolutely right. This is the first time that we have heard about the use of warrants. I think that the police rely on the common law for digital searches, but such searches are closer to searches of a house than they are to a digital stop and search. That is a closer analogy, because of the sensitive and very personal information about an individual's identity and their social relations that is held on a phone. A house search is a more accurate analogy. If we need a warrant to search a house, there should be something similar in terms of legal safeguards for digital devices. That is the first point.

The second point is that a warrant must be specific. A warrant by itself could be unlawful, as you already know. It must be specific enough to cover the reference that is mentioned; it cannot be about all the data in the mobile phone. The information in question must be relevant to the case, otherwise the taking of it would be unlawful. The issue is more nuanced than just involving a warrant. Having said that, of course there are statutory powers that allow the police to take such action. In those cases, the legality is quite clear, but there are other cases in which, in our view, it is not.

**David Freeland:** From our perspective, data protection law is quite clear that information should be obtained for a specific explicit and legitimate purpose, which should be established at the outset. If the information were to be used for some completely different or unrelated purpose, that would not comply with data protection law.

To echo the point that has just been made, one of the other principles of data protection law is that the information that is obtained must be adequate, relevant and limited to the specific purpose. In this context, that means that we should have evidence-led policing, rather than everything being obtained just in case there might be something there.

**Daniel Johnson:** Does modern technology not make that very problematic, in that once a phone has been unlocked, the whole thing has been unlocked, so it is quite difficult to say, "I am only going to look at this one bit"? Is that problematic if the police are looking through social media, for example, which is very expansive?

13:30

**David Freeland:** It potentially is. There would then be an intrusion. If the police went through all of someone's text messages, that would potentially be an intrusion into other people's private conversations that were not relevant to the case; it would not simply be a case of focusing on the conversations between the particular persons who were already of interest. If that kind of interrogation leads to other people of interest, that evidence would be of further relevance to the case, but extracting everything wholesale in that way puts the police at a risk of non-compliance.

**Daniel Johnson:** On the basis of what you have seen, are you satisfied that there is sufficient granularity in the police's thinking to deal with that?

**David Freeland:** At the moment, I want to understand the process at the cyberhub end of things in greater detail.

**The Convener:** I do not know whether Chief Superintendent McLean wants to respond to that. I am conscious that there are occasions when you might crave a warrant to search for item A and to cover item B. There are issues around that legally, of course.

**Detective Chief Superintendent McLean:** Again, it is very difficult to cover every eventuality, but the overriding principle is that the fairness of the search and how the police came by the evidence that is used against an accused will be for the court to determine.

However, I am not averse to any of the points that have been made by David Freeland and Diego Quiroz. A key aspect that we have built into the delivery of the cyberkiosks or triage devices is the issue of proportionality and necessity. There are checks and balances. The investigating officer will do an electronic submission and will check that through a supervisor, the trained officer and potentially a cyberhub. That process will be based on what matter is under investigation, what search parameters are being applied to the device and what it is that people think that they might find.

It is not just a fishing exercise. Diego Quiroz was making the point that if the search goes too wide, we would be going beyond some of our

responsibilities. If there is one matter that is under investigation, our search of the device should be appropriate. Proportionality and necessity are key. It may well be that there is a raft of evidence from other sources, including independent witnesses, so the examination of the device might not be relevant in particular circumstances. Proportionality and necessity are two key elements of the delivery of the kiosks.

**The Convener:** Question 47 in your data protection impact assessment relates to article 8. It has clearly not provided reassurance to Mr Quiroz. In response to how you would deal with article 8, on the right to respect for private and family life and the various elements thereof, the assessment says:

"As per any enquiry or investigation involving digital media there is an element of collateral intrusion. This will be managed using current and established Policy, Procedures and Practices".

Are you able to briefly expand on what—

**Detective Chief Superintendent McLean:** That relates to the point that David Freeland was making. If we take a device and we examine it, we image the whole device and we extract, download and examine all the data on that device. We then try to secure that data. We do not make it available to other officers. We look at—sorry; "consider" would be a better use of language—the sensitive material, whether it is legally privileged or journalistic, and try to mitigate the collateral intrusion, but we accept from the outset that if we are going to image the device or other parts of investigations, we will always run the risk of some collateral intrusion.

**Margaret Mitchell:** Could you comment on Privacy International's report, which suggested that police forces are using the technology in the UK without clear safeguards for the public? In particular, it suggested that Police Scotland is acting unlawfully in this area and that citizens' rights and interests are not fully protected.

You said quite clearly that, in certain circumstances, a warrant should be obtained. Are you confident that a warrant has always been obtained in such circumstances? Where is the independent scrutiny to safeguard against abuse and misuse of what you have already said could be very sensitive and personal information?

**Detective Chief Superintendent McLean:** I can answer that one. Having read the Privacy International report, I think that it gives an overview of how such technologies are being used across the UK. Different types of technology are being used, some of them are being applied differently and there are often very different sets of policies and procedures covering their use.

With regard to the assertion that Police Scotland is acting unlawfully, I would defend our position and say that that is not correct. We have not rolled out cyberkiosks, so we are developing policy and procedure around their use—I have already touched on that.

**The Convener:** You are not rolling them out, but you have trialled them and that had an impact on the public.

**Detective Chief Superintendent McLean:** Okay.

The second point was about the use of a warrant. At no point was I suggesting that we would ask for a warrant to examine a mobile device. I was saying that mobile devices will often be seized as part of a wider search that has been facilitated under the powers of a warrant. When it comes to fairness, independent scrutiny of that will take place within the court environment, where it will be considered whether the police had the powers to take the devices in question and conduct the examination that they undertook thereafter.

**Margaret Mitchell:** I am a wee bit concerned that you are saying that, ultimately, the court will decide that. I hope that the guidelines will be sufficiently robust that you will be quite clear in your mind when you go to court that there is no question of devices having been seized unlawfully. I think that there is a bit of confusion there.

If the reference group finds that there is not a sufficiently good legal basis for the police to access data, will the roll-out continue?

**Detective Chief Superintendent McLean:** The roll-out has not commenced, so it is not a question of whether it would continue, but maybe I am being pedantic. If the reference group were to raise substantive points, those points would need to be addressed. That is the whole point of the consultation.

**Margaret Mitchell:** I take it that you are assuming that the roll-out is going to go ahead. We know how many kiosks there will be. We seem to have a lot of detail, so it is a reasonable assumption that the roll-out will proceed, but if the reference group says that there is not a sufficient legal basis for accessing data in that way, will the roll-out still continue?

**Detective Chief Superintendent McLean:** If we had no legal basis to proceed, we would have to suspend the roll-out. We would have to accept that. If there was no legal basis to use the technology in Scotland, it would be inappropriate for us to continue the roll-out.

**Margaret Mitchell:** So it is essential that you work very closely with Mr Quiroz and Mr Freeland to ensure that you are absolutely clear about, and

that there is no confusion about, exactly what your powers are and that you are sure that they are being used appropriately.

**Detective Chief Superintendent McLean:** Yes. That is very much the case. We would welcome that opportunity.

**Stewart Stevenson (Banffshire and Buchan Coast) (SNP):** I want to finally nail down the issue of warrants and access to data. To do so, I will give an example. There is a court case on. As would normally be the case, the accused has been told by the court he must go nowhere near any witness. A witness sees the accused outside their house—they live on their own—using their mobile phone to photograph the house and what appears to be going on in the house. They report it to the police. I take it that the police can reasonably get a warrant to look at that mobile phone to get corroborating evidence that such activity was taking place. However, in doing so, they will look through the folder of all the photographs. If they were to find, for example, illegal images of young children, would the police be able to act on that second point as well as the first scenario that I have dealt with?

**Detective Chief Superintendent McLean:** I think that, if the police thought that they had to seek a warrant, the warrant would be to empower them to be in a private place in order to recover that device. That is the accepted principle in Scotland. They would not require a warrant to examine the phone and, thereby, the content.

The second point that you make is about self-incrimination. If the police are being proportionate and applying the rules of necessity and proportionality as they look for one piece of information within a digital examination that has a bearing on the matter under investigation but, in doing so, find something completely different, they would have some responsibility as law enforcement to bring that to the attention of prosecutors so that either other powers be afforded to them or consideration be given to a separate investigation and possible prosecution for those matters.

**Diego Quiroz:** The issue with the warrant relates to something that I mentioned before. Perhaps I was not very clear. There has to be a very specific warrant in such cases because, if you have a warrant to search a house and you go into the house and there is a folder of documentation that says “confidential”, that will not necessarily allow you to open that documentation. It is similar with a mobile phone. You can seize and confiscate the mobile phone, but examining the content or the data is a different issue. That highlights another human rights implication, which involves article 6 of the convention and fair rules of evidence. That means that proper examination of the method by which the evidence was obtained and admitted in the criminal proceedings is a matter for the ECHR and is a matter of law.

Where the evidence is of dubious quality and the rights of the defendant have not been respected, or where the evidence has been improperly obtained, the matter is for the national courts. However, that would certainly engage article 6. This is a completely different level from article 8. Article 8, article 6 and even article 10 are significantly engaged in the new policy, and they need to be rigorously scrutinised and examined before its roll-out.

**The Convener:** Mr Quiroz, are you sighted on the draft data protection impact assessment that Police Scotland has produced?

**Diego Quiroz:** I was sent the document a week ago.

**The Convener:** It says that there are no implications with regard to article 6.

**Diego Quiroz:** That is correct. I was about to say that there were further concerns on our side in relation to the impact assessment. There is no consideration of article 6 and there is no consideration of article 10, which concerns freedom of information and speech.

**The Convener:** Apparently there are no implications with regard to articles 7 and 9, either.

**Diego Quiroz:** That is correct, and, with regard to article 8, there is a heavy reliance on GDPR. There are significant concerns with the impact assessment, but we are willing to work with the police to try to help solve some of those questions.

**Fulton MacGregor:** My point has been covered—not unusually, Stewart Stevenson is a step ahead of me. However, I will ask a question from a slightly different angle, even if it runs the risk of a wee bit of repetition in the answers.

We are all quite concerned about the possibility of the collateral damage, as it has been called, of possibly private conversations between people not involved in an investigation being captured. However, let me put another angle on it—a bit like Stewart Stevenson did. If a device was being checked and a private conversation came through and another situation came to light—perhaps something that the public would expect the police to act on, such as a possible attack or something of that nature—what would be done, given how that situation had been identified? I would like the answers to that to deal with the issue in a practical sense, rather than the way in which the answers to Mr Stevenson’s question dealt with it. Just for the general person in the street, how would you proceed with that?

**Detective Chief Superintendent McLean:** Again, I do not know the specifics of the example that we are talking about, but if there was a general threat to someone's safety or public safety, I think that there is a responsibility on the police to act on that. That might be an overriding principle and whether or not that would undermine a prosecution at a later stage is perhaps a secondary issue. The overriding concern is about protecting the public. The response would very much depend on the nature of the issue. The point is that the police will often secure a warrant to search premises where they believe drugs are being supplied and, often, within those premises they will find other materials. The most routine thing that they might find is a firearm. They have a warrant to be in those premises, they have a warrant to search, but they have no power to seize a firearm. However, clearly, there is an overriding principle about public safety and potential offences—serious offences—that people have committed. At that point, ordinarily, we would seek another warrant to remove the firearm from those premises.

It is not infrequent that those types of circumstances come up, but, in terms of digital forensics, issues of self-incrimination arise less frequently. There are important checks and balances in place around proportionality and necessity that ensure that you are not taking a very wide view of all the data that is on someone's device, but are instead looking more particularly at the data that may have a bearing on the matter that is under investigation.

**Liam McArthur (Orkney Islands) (LD):** I was going to ask about the external and stakeholder groups and how they interact. We have heard that both groups have met on a couple of occasions, most recently over the course of the past week. It would be helpful to understand the frequency with which those groups are expected to meet and, indeed, the interrelationship between them. Is there commonality between them—for example, a Police Scotland presence on both? Is there any other sort of mutual membership, and what is the interaction between those two groups?

**Detective Chief Superintendent McLean:** To be helpful to the committee, I will give you a quick rundown of the stakeholders group, which is the group that might have more of a relationship with the criminal justice system, if you will. It is made up of representatives of the SPA, HMICS, SPA forensic services, the Crown Office and Procurator Fiscal Service, Police Scotland information management, the Scottish Police Federation and staff associations. I chair that group.

The reference group is chaired by our business relationship and partners lead—a Police Scotland senior civilian member of staff who has no connection with cybercrime. We have offered the position of chair of that group to attendees, and they are considering whether they would wish to take it. The people who attend are Mr Aamer Anwar, human rights solicitor and people from the Open Rights Group and Privacy International. There are invites to the Scottish Human Rights Commission—Diego Quiroz—the Information Commissioner's Office and Victim Support. The director and assistant director from the Scottish institute for policing research also attend that group.

The point that you ask about—what relationship the two groups want to have—was put to the external reference group. It wanted to retain some independence from the other group, but asked for access to the SPA member who sits on the other group so that it could report any issues that it wanted to escalate or articulate. Robert Hayes, who attends that group, is happy to facilitate that and, from time to time, at the request of the external reference group, will also attend that group.

**Liam McArthur:** In relation to Mr Quiroz's concern around aspects of article 8, you mentioned that the issue had been put to the stakeholder group and that the Crown Office and Procurator Fiscal Service had given assurances around the way that that issue would be dealt with under current practice. That suggests that the reference group will raise issues that the stakeholder group will then bat back or will decide are not issues. What is the report-back mechanism for the reference group, which presumably raised those issues in good faith and would expect a substantive answer with regard to why the concern was unfounded?

13:45

**Detective Chief Superintendent McLean:** The minutes are published and a number of actions are taken from those respective groups. We have tried to provide an overview to each of the groups about the respective meetings, so where the Crown Office makes substantive points around disclosure obligations, or where the reference group raises substantive issues around the legal basis for phones being examined, we will try to take them back to get a view from each of the groups and some of the key stakeholders and feed that back into the groups.

**Liam McArthur:** How frequent are the meetings?

**Detective Chief Superintendent McLean:** They meet almost on a monthly basis at this time, diaries permitting.

**Liam McArthur:** Mr Quiroz, what is your understanding or experience of the way in which that interrelationship is functioning?

**Diego Quiroz:** We have not attended the meetings yet. We were sent an invitation. We considered the invitation and we will attend the next meeting. At this moment I am unable to answer that specific question, but our views will be expressed in different ways, through the website of the commission, but also through different reports to this Parliament and even international bodies. As you know, we engage heavily with the United Nations.

**Liam McArthur:** I will turn back to some of the practicalities. Obviously, we have heard about the purpose of the cyberkiosks, the triage and the process whereby, if there is evidence of value to a particular investigation, that will then be passed on to the hub. Would that happen in every instance? Would further investigation be done at a more local level if evidence of value was found to be on the device, or would it at that point automatically be passed on to the hub for further examination?

**Detective Chief Superintendent McLean:** We are writing up the guidance documents covering the principles of use. There are probably only a few exceptions where devices would not go through a triage process. Those are more particularly to do with child sexual exploitation or abuse, where it might not be appropriate for local officers, in terms of their wellbeing, to look at the type of imagery involved, or they might be to do with professional standards issues, where it would be inappropriate for local officers to be involved in the investigation at that stage.

We are saying that all devices that are taken should go through the local triage process. A device will have been legally taken, we would hope. There will be a number of checks and balances, such as supervisory checks, and the device will already have been logged in police systems as a production exhibit or a piece of evidence. The triage process allows the officer at the front line to apply some disclosure principles, and in particular the test of relevance—is there anything within the device that has a material bearing on the matter under investigation? At that point, if the answer to that question that is provided by the trained operator to the investigating officer is no, the device can be returned to the owner quite quickly thereafter.

It may be interesting for the committee to know that, since I first gave evidence at the committee in early May, almost 5,000 devices have been submitted to our cybercrime hubs for full forensic examination and full download. From the figures that we are working with at the moment, we suspect that probably less than 5 per cent of them would have passed that test of relevance in terms of having anything that was materially of bearing or benefit to the investigation. Therefore a large swathe of those devices now sit within our cybercrime hubs that could probably have been returned to the owners at a much earlier stage.

The second advantage is that the officer who has taken the device, who is going to the triage operators, can quite quickly look at any material that may be relevant to the investigation and perhaps build that into an investigation or interview strategy that he or she is compiling at that time. In the absence of triage devices, that would go to a cybercrime hub and it is likely that it would be a number of months before the investigating officer would get any response about what may or may not be on that device. Therefore it provides a much better service at the front end to the investigating officers and I think that it provides a much better service to the public

More particularly, and echoing some of the contributions made here today, there is a risk with the amount of data that we are downloading and examining from devices, which is needless. It is all about a process. The overriding principle is that these triage devices do not extract or store any data on them; what they do is provide an opportunity to apply the test of relevance and see whether or not the device needs to go any further in the criminal justice process.

**Liam McArthur:** We have heard examples earlier about child pornography, and the duty or expectation on officers to follow up such leads, but there will be examples that are considerably less serious but may still fall foul of the law in some way. I suspect that there will be public anxiety that, although a phone is being taken and scrutinised for one purpose, there is a risk of self-incrimination spanning a wide range of fairly minor misdemeanours that would still be counted as offences. What assurances can you offer about collateral impact and the proportionality of the use that is being made?

**Detective Chief Superintendent McLean:** I have talked through some of the processes in terms of the supervisory checks, using the rules of proportionality and necessity, so that starts at the very initial point, when the device is seized and there is an electronic submission through the cybercrime process.

**Liam McArthur:** At the moment, what you have is a hub process. I understand the issues with the delays and the time taken to carry out investigations and return devices to individuals, but the flip side is that you will have far more officers and possibly also civilian staff in a position where they will be interrogating devices and will be required to be trained in that. Their use of discretion may vary. Therefore, you will have officers who are absolutely on the money in how

they apply the protocols, but there has to be a heightened risk of officers being less able to interpret the protocols in a way that the public would expect, so concerns will arise. Just by dint of spreading out the numbers of individuals who will have to be trained and then implement and act within the protocols, there has to be a heightened risk.

**Detective Chief Superintendent McLean:** I accept the points that you make, but I think that the key word that you used was "discretion". Discretion is at the disposal of officers at this time. I suppose that, if we are thinning out the volumes that go to the cybercrime hubs and the number of examinations, we are thereby reducing the risk and the potential for those numbers. I know that you are saying that the numbers are at the front end, but there is discretion available to officers to decide that matters are fairly minor. It is difficult to give an explicit position, as it would depend on the severity of the crime or the information that they have come across. I do not think that there is necessarily additional risk. I think that risk is ever-present; it is here at this time and is dealt with by way of discretion. It is open to the police.

**Liam McArthur:** The risk comes from the fact that, as you have accepted, the exposure to a vast amount of data means that there is more potential for information to come to light that would then require an exercising of discretion that does not happen to the same extent now. I appreciate that all officers will have a level of discretion and we would not want it otherwise. You need to trust them to act with a degree of common sense and proportionality, but that exposure to a vast amount of data leaves open a wider risk that that discretion will be exercised in a less proportionate fashion.

**Detective Chief Superintendent McLean:** I have one final point, convener—I am conscious of your time and I will try to keep this very short. Currently, the process is that we go to a cybercrime hub, there will be a full examination and all the data will be pushed back for the investigating officer to make that determination. I think that that affords them a greater opportunity to look at self-incrimination across all the data. The process that we are looking to introduce is that the investigating officer will ask the trained officer to use very closed search parameters in examining the device and to come back with, in effect, a positive or a negative response. That amount of data is closed off in many respects to the investigating officer and therefore the risk is reduced.

**Liam McArthur:** Mr Quiroz, did you want to say something?

**Diego Quiroz:** Training is a very important point. As far as we know, there are 18 police officers trained. We do not know what the type of training is. Most privacy protocols fail because it is not a technical question; it is a human question, as you said, so the people who are exposed to that information are individuals. It is not a machine. I think that training is a very fundamental question.

The other point is that, obviously, there are good reasons to interfere with the right to privacy. Article 8 foresees those reasons—prevention of crime, national security and so on—but we think that, without independent oversight, clear guidance and examination of the pressing social need to introduce this measure and the proportionality of the measure, there is a higher risk of it being arbitrary or subject to abuse. We think that some of those questions are still unanswered.

**David Freeland:** I echo that. A lot of the internal governance around the use of these devices is crucial. It is crucial that there is proper guidance on what to do, that there is proper training and that there is internal oversight as well as external oversight of this, by way of audit sampling and ensuring that officers know what they are doing and that training is not a one-off at the start. If training needs arise through audit or whatever, those need to be addressed at an appropriate stage as well.

**Stewart Stevenson:** I just want to engage with some of the numbers. The first question is this: how long does the triage take?

**Detective Chief Superintendent McLean:** It would probably depend on the type and complexity of the device.

**Stewart Stevenson:** Broadly how long does it take?

**Detective Chief Superintendent McLean:** I will go to my technical expert, Peter Benson, to answer that for me.

**Peter Benson (Police Scotland):** All devices are different. The triage system, much like the software that is used in the lab, will prompt you to do certain things. If it is what we all understand as a burner phone, which is a phone that is not a smartphone, does not contain very much and may only have the stuff on the SIM card, that is going to be very quick.

**Stewart Stevenson:** What does "very quick" mean?

**Peter Benson:** Very quick could be less than an hour.

**Stewart Stevenson:** And a more complex one?

**Peter Benson:** If it is an iPhone, then, depending on the size and how much data is on it—and I think that we all know from yesterday that one is going to be released that is absolutely enormous in terms of storage capacity—that can

take up to two or three hours. It still has to go through the system. In the triage system, you are going to set parameters that narrow down the field of what you look at.

**Stewart Stevenson:** That is useful. That leads me to my real question: is triaging done in the hubs currently? Because if 90 per cent of what you are getting in is ultimately found to be of no interest, are you triaging to try to find that 90 per cent earlier on now?

**Peter Benson:** We do not triage in the hubs.

**Stewart Stevenson:** Why?

**Peter Benson:** You know the level of submissions that we have. If I run several phones through and produce something else for someone to review, that lets me process more phones, so there is maybe an element of sausage factory and throughput.

14:00

**Stewart Stevenson:** If the maximum is three hours, that means that each of the 41 devices will be in use for triage for 30 hours per month—that is what the numbers tell me. It strikes me that you are trying to get the things that are not worth dealing with out of the way first, which is good news. Is there an implication that the number that go to the hubs—currently, it is 5,000—is constrained by the present arrangements and that you would expect that more than 5,000 would go through the triage system but the number that go to the hubs would reduce? Is that where we are headed?

**Peter Benson:** Absolutely. The pressures on the hubs are matters of volume. We have to satisfy the needs of procurators fiscal, who will give deadlines for things that they want. That has to be one of the first things that we do.

**Stewart Stevenson:** We are running out of time, so I want to try to be crisp. Really, we are trying to do two things with the devices. First, we want to return phones that are of no interest much more quickly and get that out of the way. Secondly, we want to get to the hubs a greater number of serious cases that can be properly and fully analysed so that we improve law enforcement where a mobile phone is part of the equation.

**Peter Benson:** Absolutely.

**Detective Chief Superintendent McLean:** The figure of 5,000 that I gave is what we would expect for a four-month period. I have previously given evidence to the sub-committee that we are on track for about 15,000 devices a year, which is based on the numbers over the past couple of years. The 5,000 is an indicative figure for a four-month period, and we would expect to see 15,000 in the course of a year.

**Stewart Stevenson:** Right, but the principles that I articulated remain the same.

**Detective Chief Superintendent McLean:** Yes. As soon as we get to the cybercrime hub, we are into full examination, joint reports and the criminal justice system.

**The Convener:** What is the status of the individual while their phone is being triaged for an hour?

**Detective Chief Superintendent McLean:** It depends on the circumstances of the police contact with the individual. They may be an accused person and have been arrested or they may have been a witness to an incident and have provided their phone, or the police may have taken it under a common law power. It very much depends on the circumstances.

**The Convener:** Is that following the change to the process?

**Detective Chief Superintendent McLean:** Yes.

**The Convener:** Are those the only two statuses that someone could have?

**Detective Chief Superintendent McLean:** They could be not officially accused or they could be officially accused.

**The Convener:** Or they could be a witness.

**Detective Chief Superintendent McLean:** Yes.

**The Convener:** Alternatively, do you include someone who is not officially accused as being a witness? I am not being pedantic with words. The concern is that there is potential for some huge fishing exercise. I know that you will say that you have neither the time nor the energy for that, but the concern is that someone becomes involved in something and perhaps finds themselves in a police station, and there is an opportunity to look at their phone. Their status at that moment—never mind the status of the inanimate object—is very important.

**Detective Chief Superintendent McLean:** I have described the legal basis on which the police could take a device, and I do not think that there is any change to that. The criminal justice legislation has provided a distinction between someone having had their liberty taken away from them and someone having been arrested. A person has been deprived of their liberty at that stage, whether or not they are officially accused.

**The Convener:** The reason why the term “witness” is important is to do with the earlier discussion that we had about your remarks about the Crown determining that something is an

operational police matter were a witness to withdraw their wish to have their phone examined.

**Detective Chief Superintendent McLean:** A witness is very different from someone who has been arrested.

**The Convener:** Indeed.

**Daniel Johnson:** I want to follow on from Liam McArthur's points about training. Mr Quiroz and Mr Freeland said that training is important. Based on what you have seen from Police Scotland so far, will the training be sufficient? Have you had any sight of that?

**Diego Quiroz:** The quick answer is no, unfortunately. Mr Freeland explained the importance of continuous training. It is important that there is training, that its scope includes human rights as a key element and that it then continues.

**Daniel Johnson:** I want to go back to Mr McLean. It is now September, and you are seeking to roll out the kiosks in November but, from what we have heard, there still needs to be resolution around the legal framework principles and particularly on human rights. That has not been done or is not yet concluded. Surely you need that to be concluded in order to devise the training that needs to take place. You have seven or eight weeks to conclude those legal and human rights principles, devise the training and deploy the training. Is that enough time to do all of that?

**Detective Chief Superintendent McLean:** I accept that we are being extremely ambitious. The training has been devised and written up. You are right that the timeframes are ambitious, but I go back to my earlier point that we understand that the roll-out can be done only once we have concluded all those other matters.

**Daniel Johnson:** How on earth can you devise training prior to concluding the work on the human rights basis upon which you will be carrying out the work? I struggle with that in quite a fundamental way.

**Detective Chief Superintendent McLean:** I apologise, as I should perhaps have been a bit more explicit on that. I mean the training on the operation of the devices. I hope that we are building on a knowledge base. Police officers are not coming to the issue blindly. We are building on our understanding of proportionality and necessity, our legal powers and our responsibilities under the articles. However, you are absolutely right that the document sets that will support the delivery need to be concluded, and we have set ambitious timescales for that.

**Daniel Johnson:** At what point does that ambition become overambition?

**Detective Chief Superintendent McLean:** We remain optimistic, but we understand that there is a lot of work to be done.

**Fulton MacGregor:** Police Scotland has stated that downloading data from devices on to disc might be an option. Is that still being considered? Has a solution for encrypting discs been found?

**Detective Chief Superintendent McLean:** The technology that we have procured has the ability to export data, but we have taken a conscious decision not to export any data on to disc, which has been welcomed by the groups that I have mentioned. The position is that the devices will not extract data, store data or export data on to disc or any other format.

**Fulton MacGregor:** What is the reason for that decision?

**Detective Chief Superintendent McLean:** It is primarily about data security and privacy. As soon as we export data, we need to consider a range of audit and compliance issues. As part of the on-going review, we will see whether there is an evidence base but, in the absence of that, we are not going to put that process in place at this time.

**The Convener:** The committee is keen to understand police operations and ensure that there is support to tackle crime but, to go back to a comment that I made at the beginning, the process is completely back to front. There has been significant public expenditure—curiously, it is just short of the amount that would trigger involvement by the Scottish Police Authority—and work was undertaken with no assessments. We want an assurance that that will not be the way that you go about business henceforth and that you will engage meaningfully with Mr Freeland, Mr Quiroz and others on the wide-ranging concerns that remain about the process, notwithstanding the work that has been done. We welcome the engagement, but do you understand the depth of concern?

**Detective Chief Superintendent McLean:** Absolutely, convener, and I will give you that assurance. That is why I have personally become involved in a number of the groups. I hope that Mr Freeland and Mr Quiroz will participate and will see the openness and transparency that we are trying to bring to what is a complex issue. It is wider than just cyberkiosks; there is a wider piece around digital forensics for law enforcement. There are absolutely lessons that are learned, and I can give an assurance that in future our approach to those challenges will be more considered.

**The Convener:** We hear about the additional technology that is en route and the additional capacity. Just to follow on from my colleague Margaret Mitchell's comment, will you reaffirm

that, if you fail to get the approval of Mr Quiroz and Mr Freeland as regards the serious human rights and legal aspects, you will not proceed?

**Detective Chief Superintendent McLean:** Yes. I am on record as saying that, if there is no legal basis for us to continue with the technology, it will not proceed.

**The Convener:** Thank you very much indeed. I thank you all for your written evidence and for attending. It is much appreciated.

We now move into private session.

14:10

*Meeting continued in private until 14:14.*

Published in Edinburgh by the Scottish Parliamentary Corporate Body, the Scottish Parliament, Edinburgh, EH99 1SP

All documents are available on
the Scottish Parliament website at:

www.parliament.scot

Information on non-endorsed print suppliers
is available here:

www.parliament.scot/documents

For information on the Scottish Parliament contact
Public Information on:

Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

The Scottish Parliament
Pàrlamaid na h-Alba