OFFICIAL REPORT
AITHISG OIFIGEIL

Justice Sub-Committee on Policing

Thursday 10 May 2018

Session 5

The Scottish Parliament
Pàrlamaid na h-Alba

Thursday 10 May 2018

CONTENTS

JUSTICE SUB-COMMITTEE ON POLICING
6th 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)
*Rona Mackay (Strathkelvin and Bearsden) (SNP)
*Ben Macpherson (Edinburgh Northern and Leith) (SNP)
*Liam McArthur (Orkney Islands) (LD)
*Stewart Stevenson (Banffshire and Buchan Coast) (SNP)

*attended

THE FOLLOWING ALSO PARTICIPATED:

Detective Superintendent Nicola Burnett (Police Scotland)
Kenneth Hogg (Scottish Police Authority)

CLERK TO THE COMMITTEE

Diane Barr

LOCATION

The David Livingstone Room (CR6)

Scottish Parliament

Justice Sub-Committee on Policing

Thursday 10 May 2018

[The Convener opened the meeting at 13:00]

Decision on Taking Business in Private

The Convener (John Finnie): Feasgar math, a h-uile duine, agus fàilte. Good afternoon, everyone, and welcome. This is the sixth meeting of the Justice Sub-Committee on Policing in 2018.

We have received no apologies. Our colleague Liam McArthur is in the chamber at the moment debating a constituency issue, which also concerns my constituency, so I hope that he is debating it well. He will join us at some point.

Agenda item 1 is a decision on taking business in private. Do we agree to take in private item 3, which is a discussion on the sub-committee's work programme?

Members *indicated agreement.*

Digital Device Triage Systems

13:01

The Convener: Agenda item 2 is evidence on Police Scotland's proposed use of digital device triage systems, which are more commonly referred to as cyberkiosks. I refer members to paper 1, which is a note by the clerk, and paper 2, which is a private paper.

I welcome to the committee Detective Superintendent Nicola Burnett from Police Scotland, and Kenneth Hogg, who is the interim chief officer at the Scottish Police Authority. I thank the witnesses for their written submissions which, as ever, are helpful. As it is Mr Hogg's first appearance before the sub-committee, I invite him to make a short opening statement.

Kenneth Hogg (Scottish Police Authority): Thank you, convener. I am pleased to have the opportunity to contribute to the sub-committee's discussions for the first time since taking up my role as interim chief officer of the Scottish Police Authority.

At various stages, Police Scotland has briefed the authority about its proposals to use cyberkiosk devices. That engagement has been part of the authority's oversight of delivery of the policing 2026 10-year strategy. The kiosks are one of 70 initiatives that comprise that wider programme of change.

The authority has asked Police Scotland about implications for data handling that are associated with cyberkiosks. A key assurance that Police Scotland has provided is that the new technology does not extend the powers that the police already have in relation to accessing information on mobile phones. Instead, it lets officers do what they already do more quickly and more locally.

Public interest in handling of personal data is of growing importance to policing as it adapts to working in an increasingly digital world. Therefore, the SPA is increasing its oversight of such issues, including through its scrutiny of an integrated data, digital and information and communication technology strategy that Police Scotland is developing. More generally, the SPA is also undertaking a comprehensive programme of improvement in its own ways of working. That includes becoming better able to scrutinise Police Scotland's delivery of its change and modernisation programmes, and to shine a light on issues that are of public interest.

I look forward to answering the committee's questions.

The Convener: To start the questions, I refer to a submission that the sub-committee received

when it was considering Police Scotland's standing firearms authority. Iain Whyte, who is an SPA board member, addressed the committee. In the submission to the committee, we heard:

"One of the principles of good governance is that the public voice is appropriately heard within decision-making."

In relation to the standing firearms authority, the SPA stated that one aim of its inquiry was to assess

"what, if any, lessons might be learned around how operational decisions with wider strategic or community impact are communicated to national and local oversight bodies and other key interests."

Is Mr Hogg or Ms Burnett able to outline what public engagement there has been on use of cyberkiosks?

Kenneth Hogg: The proposals to introduce cyberkiosks are, in the first instance, part of a national cybercrime technical strategy. That, in turn, forms part of the policing 2026 10-year strategy. There has been public engagement on the overall strategy. The SPA has had conversations with Police Scotland at various stages over the past several years about the development of cyberkiosks. Some of those conversations have been public and some of them have been in private.

The Convener: You will understand that the issue is very much in the public domain now. Are you able to say how much has been spent on the initiative?

Kenneth Hogg: Yes. The purchase of the 41 cyberkiosks comes to a total of £445,000, including VAT. That includes the cost of licences and training. In addition, there will be a continuing revenue cost of £100,000 a year associated with their use.

The Convener: Are you, or is Ms Burnett, able to explain what

"Evidence Management System Support and Maintenance"

is about? I understand that a contract for that has been awarded to a company called Abbott Informatics.

Detective Superintendent Nicola Burnett (Police Scotland): I am sorry, could you repeat that, convener?

The Convener: Yes. The term is:

"Evidence Management System Support and Maintenance".

There is a contract for that worth £431,000 with Abbott Informatics. How does that relate to the issue that we are discussing?

Detective Superintendent Burnett: There is no direct link between that and procurement and deployment of kiosks, as far as I am aware. I do not know for sure, but I think that that contract is to do with management of information within the cybercrime hubs. I will need to get back to the committee to confirm that.

The Convener: So, if I understand you, that contract might subsequently have some relation to information that the kiosks glean.

Detective Superintendent Burnett: No. It might have something to do with the overall digital forensic infrastructure that is managed within the cybercrime hubs. However, the information that is managed in the kiosks is managed solely within those devices. No data is retained on the kiosks once an examination has taken place.

The Convener: If data is uncovered as a result of the examination, what happens to it?

Detective Superintendent Burnett: Perhaps it would help if I explained how we propose in our policy, practice and procedure to use the cyberkiosks, as they are colloquially known, in our local policing areas.

If a digital device is seized for a lawful policing purpose and we are trying to identify whether there is data on it that could expedite or support the inquiry that is under way, that device will be inserted in the cyberkiosk by one of our specially trained officers. Thereafter, we can put in parameters for our search. For instance, if we were looking specifically for text messages to support a domestic abuse inquiry, we would be able to put in specific search parameters to identify whether the device held such information. If that was the case, we would confirm that the device contained information that would support the inquiry, then send it to one of our Police Scotland cybercrime hubs for full digital forensic analysis.

The Convener: The contract was awarded close to the awarding of another, which is why the question has arisen. Is that when the evidence management system support and maintenance would kick in?

Detective Superintendent Burnett: I will need to go back and get confirmation on that contract.

The Convener: Okay. Another contract, worth £286,000, was awarded the same day for e-discovery and analytics software to be provided by a company called Nuix. How does that relate to the cyberkiosks?

Detective Superintendent Burnett: That is another piece of software that is being procured for the establishment and finalisation of the digital forensic hubs that are being stood up within Police Scotland. The purpose of the digital forensic hubs is to ensure that, in the north, east and west of the country, we have a systematic and corporate hub system that supports digital forensic analysis of

devices that are seized by Police Scotland. Items that have been purchased this year, including the Nuix software, are tools that will be stood up within the hubs to assist us in our digital forensic analysis of devices that are seized.

The Convener: The figure that Mr Hogg mentioned is £75,000 more than the figure that I have, but the cumulative total for the contracts is £1,087,000. What input did the Scottish Police Authority have on that expenditure?

Kenneth Hogg: To clarify, the figure that I gave includes VAT—that is the difference between the £370,000 figure, which is cited in the written evidence, and the figure that I gave.

The cyberhubs that are being described are part of the national cybercrime technical strategy, which I mentioned earlier. The strategy is to create three centres of expertise across Scotland to increase and modernise Police Scotland's ability to deal with all forms of cybercrime.

Decisions on procurement and expenditure take place within the agreed system of financial governance between the SPA and Police Scotland. Police Scotland can undertake, at its own hand, purchases up to a certain value. Purchases that are over that threshold—£0.5 million—need to come to the SPA for my approval, as the accountable officer for the entire policing budget. Beyond that, such purchases need to go to the SPA board and, indeed, to the Scottish Government for approval.

The purchase of the 41 cyberkiosks fell within the category of expenditure that Police Scotland can procure at its own hand. The business case for that expenditure went through Police Scotland's governance procedures and boards, including the capital finance and investment board and the change board. That process happened in 2017, before procurement in 2018.

The Convener: Clearly, the cumulative cost of the three contracts goes over that threshold, and we have heard that two of the contracts are linked. How do you monitor that from a governance point of view? For argument's sake, let us say that there are lots of contracts, each costing £499,000. I think you know where I am going with that.

Kenneth Hogg: To my knowledge, the additional pieces of expenditure to which you have referred are separate from operation of the cyberkiosks. The contracts might all operate within the cyberhubs, and be part of the national cyber capability, but they are separate.

In terms of oversight, the SPA has access to and attends meetings of Police Scotland's capital finance and investment board and of its change board, which approves business cases. The SPA is sighted on expenditure, even if the expenditure falls below the threshold at which it formally requires SPA approval.

The Convener: Were you aware of each of the contracts?

Kenneth Hogg: No—I was not involved in discussions about those particular contracts.

Stewart Stevenson (Banffshire and Buchan Coast) (SNP): I want to go back to Detective Superintendent Burnett and make sure that I have understood some of the things that were said. My first question is the simple one. I take it from what you said that data that is extracted from a device that has been seized and analysed on the kiosk, for the purpose of triage, never leaves that kiosk.

Detective Superintendent Burnett: No—and the data does not remain on the kiosk. When we insert the device, we have a view of any data that is held on the device. We then identify whether the device contains anything that is pertinent to the investigation that is under way, and if it does, the next stage is to submit the device for full digital forensic analysis. If it does not, the device will be returned in due course to its owner. However, at the end of an examination on the cyberkiosk, that examination is closed down. Any data that was viewed through the window of the kiosk will not remain on the kiosk device, but a clear audit trail will remain. There will be a unique reference number, so we will have a form of audit and governance that understands when activity has taken place, but does not retain data that was viewed on the device.

13:15

Stewart Stevenson: The other side—you have partially answered this—is that all the data from a device that has been seized is extracted in the central facility, and associated processes govern the use of, and protection of access to, that data. If that is the case, you can just say yes.

Detective Superintendent Burnett: Yes. However, another option is available to trained officers. If, while viewing the data on the kiosk, there is an opportunity to download data that is of consequence on to a disk, they can do so. We are looking at how we will manage that.

To be clear, the kiosks are not in operation at this time. The deployment part of a project is always at the end of procurement. We have to consider training, policy, practice and procedure, as is right and proper with any technologies that we bring into Police Scotland.

Although downloading data on to a disk is an option, we are looking at the solutions for how those disks can be encrypted. We have yet to be fully satisfied that that will be a workable option, but it is under consideration.

Stewart Stevenson: I do not want to go too far on this point, but would that happen only with a device that had been triaged and found to be a device in which you would take further interest?

Detective Superintendent Burnett: That is correct.

The Convener: If I have noted this correctly, you have twice used the phrase "policy, practice and procedure". I would have thought that you would have wanted to clarify all the requirements before you undertook trials in which you accessed 195 phones and 262 SIM cards in Edinburgh and 180 phones in Stirling. Will you outline the legislative framework under which you have done that? I appreciate that there may be a number of overlaps. Where does independent oversight of that practice lie? What were the parameters of your trial?

Detective Superintendent Burnett: Are you referring to the legal framework under which we have the power to use the device?

The Convener: Under what authority can you take possession of a phone, interrogate it and retain its data? Who has access to that data? How would it be disposed of?

Detective Superintendent Burnett: On the first point, there are, in general terms, four legal frameworks—for want of a better phrase—under which we could bring a device into lawful custody. That, of course, would be required to be for a policing purpose.

There are powers under common law. Perhaps it would be helpful if I gave a scenario for each of the elements, because that might—

The Convener: Are you saying that anyone who is arrested under common law could have their phone taken into possession?

Detective Superintendent Burnett: Yes, or—

The Convener: Would that include for breach of the peace?

Detective Superintendent Burnett: Police could seize a person's mobile phone or other device if the person is under arrest. Thereafter, their phone could be inspected. I was about to give a different example. If a person poses a high risk—if there was clearly a threat to life, for example—we would consider looking at their mobile phone.

We also have powers that exist under a warrant. We could be provided with a warrant under the Misuse of Drugs Act 1971, for example, that would give us the relevant powers.

The third element is statutory powers. Again, I will use the Misuse of Drugs Act 1971 as an example. A person who is detained under section 23, on powers to search and obtain evidence, could have their phone examined.

The fourth element is when, for example, a victim of crime—whether it be sexual or domestic, for example—provides their device voluntarily for examination and there might be information that is pertinent to the inquiry on that phone.

The Convener: I have a rough figure here. My sums are not that good, but if we add 195, 262 and 180, that makes well over 630 devices having been examined by Gayfield Square police station in Edinburgh and by police in Stirling. How many warrants supported interrogation of devices?

Detective Superintendent Burnett: Unfortunately, I do not have that information.

The Convener: Do you have a ballpark figure?

Detective Superintendent Burnett: No, I do not. That information was not retained during the proof of concept for the devices.

The Convener: Why not?

Detective Superintendent Burnett: From what I have been led to believe, during the pilot that took place in 2016, the devices were trialled in two areas so that we could better understand how front-line officers would react to and be able to use them. As part of the proof of concept, specific officers were trained in using the devices and were provided with training information that let them understand the framework that we have just discussed—that is to say that, prior to being inserted in or examined on a kiosk, a phone had to have been seized for a lawful policing purpose. If officers were not satisfied that those parameters had been met, at that time there would have been no reason why we would have examined a phone on a kiosk.

The Convener: What advice was given to the owner, or the person in possession of, the phone about their rights with regard to seizure?

Detective Superintendent Burnett: Again, as far as I am led to believe, no specific advice was given to individuals. Obviously, I am not aware of the specific conversations and interactions that occurred during each phone seizure, but I can say that, most of the time, if a phone had been seized by the police, its owner would have been aware of that by virtue of having been present. However, I appreciate that that would not have applied all the time. We would have seized a phone for a lawful policing purpose, so there would have had to be some form of understanding that that was why we were doing so. However, as far as I am aware, no specific information would have been provided.

The Convener: In the two trial areas, how many people came into custody whose phones were not seized?

Detective Superintendent Burnett: Again, I cannot answer that question.

The Convener: Is that not vital information? Would you not have wanted to know the percentage if it might have helped to gauge future workload? Would you not have wanted to know the percentage of people who came through the door whose phones were seized?

Detective Superintendent Burnett: As I have said, at the time, the trials were about proof of concept and about understanding the technology and how it would be reacted to and used by front-line officers. On that point, I will say that the devices that were examined were ones that officers had seized for a lawful policing purpose and felt that they either clearly had, or were suspected of having, something on them that would support the officers' investigations.

The Convener: Could you try to get the additional information that has been requested?

Detective Superintendent Burnett: Yes, convener—I will try.

The Convener: I could spend all afternoon asking questions, but I am not going to do so. Before I pass the questioning over to other committee members, I want to ask whether any human rights or community impact assessments or risk assessments were done on the trial. I think that the committee asked that they be made available to us. Do you have any of those?

Detective Superintendent Burnett: They are on-going.

The Convener: On-going?

Detective Superintendent Burnett: Human rights and equalities impact assessments and a data impact assessment are on-going. As I have said, at this moment, we have procured the kiosks but have not yet rolled them out, so the assessments are on-going as part—

The Convener: So, the trial took place without any of those assessments having been made?

Detective Superintendent Burnett: I would need to confirm whether they occurred at the time. I am unaware of that.

Daniel Johnson (Edinburgh Southern) (Lab): I just want to establish something. You have said that the kiosks were trialled to assess the usability and usefulness of the technology, and that it is only subsequent to the trial that the procedures are being put in place and the human rights impact assessment is being carried out. What about the procedures for people who were using the kiosks as part of the trial and, indeed, the question of human rights? You were trialling the kiosks in Edinburgh, where my constituents might have come into contact with their use, and I am surprised that none of those matters was thought about in relation to the trial's parameters. Would it not have been seen as important to put in place the right procedures and to carry out a human rights assessment for people who might have their phone seized as part of the trial?

Detective Superintendent Burnett: Absolutely. I understand the points that you make. However, I need to confirm whether an assessment was completed in 2016, as I do not know.

Daniel Johnson: You do not know.

Detective Superintendent Burnett: I do not know.

Daniel Johnson: Would it be of concern if no consideration had been given to that as part of the trial?

Detective Superintendent Burnett: That is something that I will need to go away and confirm. However, I can say that the issue was discussed as part of the training during the test case in 2016. The input to the officers who were being trained was that a device had to be seized under a lawful policing framework prior to any examination.

Daniel Johnson: I ask you to clarify the data that the kiosks allowed officers to access. Given that, these days, mobile phones can capture everything from where a person has been through to their walking gait, their relationships and their social status, what would officers have been able to see and access by using the kiosks as part of the trial?

Detective Superintendent Burnett: The best way that I can describe it is that a kiosk is like a window on to the device that is being examined. Any data that is held specifically on that device can be viewed via the kiosk.

Ben Macpherson (Edinburgh Northern and Leith) (SNP): My supplementary question is related to Daniel Johnson's question on the preliminary work that was done. Like Mr Johnson, I am an MSP for Edinburgh—my constituency is Edinburgh Northern and Leith. I am concerned about the lack of preliminary work and the fact that the position cannot be clarified at this point. What was done to inform people who came into contact with officers that the trials were taking place, and to raise general awareness? Can you confirm whether a communications campaign took place or whether people were informed when they interacted with Police Scotland?

Detective Superintendent Burnett: No specific communication was made, because the technology is not new—it has been available to United Kingdom law enforcement since the 1990s, and it has been made available to and used by Police Scotland since the force started. The difference is that, due to advances in the

technology by 2016, we were able to provide the facility at the front end. However, the policy was not different and Police Scotland was not doing anything different, so no specific communication was made.

Ben Macpherson: If an individual was detained at, say, Gayfield Square police station, how would they have been informed that the process was taking place on their device?

Detective Superintendent Burnett: It would not necessarily follow that there would have been a specific communication regarding that. Not everybody who is arrested has their device seized and thereafter investigated. When we seize a device for a lawful policing purpose because we think that there is potentially some information on it that would support an inquiry, the device then becomes a piece of evidence, after which, once it is in the evidential chain, it will then be viewed via the kiosk.

Ben Macpherson: My general experience of working with Police Scotland in Edinburgh is that its headquarters at Fettes is very good at informing local MSPs about changes that are taking place. I cannot recall receiving any correspondence on this. Perhaps that is because it happened in early 2016, and therefore before my election, but it would be good to know whether any effort was made to inform elected members, who might have received correspondence from constituents about it.

Detective Superintendent Burnett: I can certainly check that, but I anticipate that, for the reasons that I have just mentioned, the answer will probably be the same. The technology was not new for Police Scotland. We had been using it, and the only difference was that we had the opportunity to roll it out further to expedite inquiries. In future, we hope to get devices back to people more quickly if they do not contain information to support those inquiries. By doing so, we can more quickly get the devices that have pertinent information on them to our hubs for processing and so provide a better service to the public.

13:30

Ben Macpherson: On that operational point, there are instances in which both people who have been charged and victims of crime have had their mobile phones taken away from them for significant amounts of time while cases progress. Is there an operational policy intention for this initiative to have an effect on that?

Detective Superintendent Burnett: Absolutely. The whole point of putting kiosks at the front end is the opportunity that it gives us to triage devices, so that only those that are of significance in supporting an inquiry end up being processed and submitted for digital forensic analysis. At the moment, it can take up to eight months for a device to be examined. If we can do anything to expedite that by using a triage facility, we have an opportunity to give a better service to the public. If we decide that a phone holds significant information that will support the inquiry, it goes into the hub, or if we decide that it does not, it needs to go back to the owner, whether they are a victim, a suspect or an accused person.

Margaret Mitchell (Central Scotland) (Con): Good afternoon. My first questions are for DS Burnett. The vulnerable persons database has been in operation across Police Scotland since March 2014. I hope that you realise that there are significant concerns about the retention of data and the appropriateness of what is retained. Can you confirm whether individuals who are classified as being of no concern and to whom the VPD is not applicable are recorded in the VPD?

Detective Superintendent Burnett: Unfortunately, I will have to defer to others to answer that question; it is not my area of business.

Margaret Mitchell: It is pretty germane to how Police Scotland collects data and its policy for retaining data. Are you not familiar with the vulnerable persons database at all?

Detective Superintendent Burnett: I am aware of the interim vulnerable persons database. I have not used it for a significant period of time. I work in the specialist crime division, and it is not a database that I am proficient in using at the moment. It would not be right for me to answer that question, because I cannot confirm the position.

Margaret Mitchell: I can perhaps ask the SPA, since the issue goes back to 2014. I am led to believe that a significant proportion of the entries are classified as being of no concern or not applicable. That led the Information Commissioner's Office to question why information was collected in the first place, if entries fall into those categories. Should the SPA be aware of that? Is it aware of it?

Kenneth Hogg: I do not have specific information about that particular database, but the SPA is now upping the level of scrutiny and engagement around the whole area of digital data and ICT. Police Scotland is in the process of developing a new strategy to bring together ICT and the use of data and digital technologies. It has reached the point of producing a strategic outline business case. We will discuss that at the SPA board meeting on 31 May. We expect that work to be developed into an outline business case by the autumn, and for the SPA to engage with that.

Margaret Mitchell: Right. Do you see my difficulty? This is about collecting data from mobile phones and assessing what is relevant and what is not relevant. Is there a shift in policy? Is there a deletion policy? You have no idea how the vulnerable persons database is working. Surely the very first question that you should be asking is how you retain data and what the policy is just now. If you cannot answer that question, perhaps you can answer a question on the proposal to purchase iris recognition technology. Are you aware of that proposal?

Kenneth Hogg: Yes, the SPA is aware that Police Scotland is considering that proposal. I do not have the details; perhaps DS Burnett can provide them.

Margaret Mitchell: It is concerning to note that there is no legal basis for the collection of custody images but, apparently, there are currently 1 million of them. It concerns me that, in your evidence, DS Burnett, you say that you will test some policies out after procurement. What is being stated here? Is it the intention, before the new technology is purchased, to establish a code of practice that covers the existing content of the database, whether it is legitimate to hold that information, whether there is a deletion policy and whether there is a shift in policy for emerging data and any future data? The code of practice should be established before there is any question of purchasing the equipment. An answer from both of you would be helpful.

Detective Superintendent Burnett: We are still working our way through the policy, practice and procedure for the kiosks. However, Police Scotland has data retention policies. The policies for any data that is held in the digital forensics hubs and anywhere else are 12 years plus one for serious crime, and six years plus one for other crime. However, to be clear, no data is retained in the kiosks.

Kenneth Hogg: The key point is that there is no shift in policy. As far as the SPA is aware, the kiosks do not allow the police additional powers beyond those that they already have and what they already do. Instead, they enable devices that do not need to be sent to the specialist hubs for a full forensic digital download not to be sent in the first place.

Because the kiosks are available in local police stations, people whose phone is handed over to the police as part of a lawful policing purpose can have their phone examined there and then and the police can determine there and then whether the phone requires to be sent off for a full download. The benefit of that is not only that an individual, who could be a suspect, a witness or a victim of crime, gets their phone back more quickly but that we lessen the backlog stacking up in the digital hubs of devices that require a full download because there is a more serious potential offence at the bottom of the inquiry.

Margaret Mitchell: I will put it another way. Data will be extracted from the device. You say that it is not kept in the kiosk, DS Burnett. That is how it is supposed to work. The vulnerable persons database is supposed to work very differently from how it works now. It has attracted the attention of the Information Commissioner's Office, if not the SPA, which is the oversight body, ironically. Has the ICO been involved? Have you been contacted about the proposals for the kiosks, the use of iris recognition technology or any other data protection issues?

Detective Superintendent Burnett: I have not had any direct contact with the Information Commissioner's Office on the kiosks. However, as part of the finalisation of our policy, practice and procedure, we plan to organise a demonstration event to which we will invite parliamentarians—including sub-committee members, if you wish to come along—as well as Government officials and others from the SPA who have not yet seen the kiosks.

We also plan to establish an external reference group. That is really important. The points that have been made in this meeting reinforce our need to have that group to ensure that we give an opportunity to, and take expert advice from, people outwith Police Scotland. That will mean that we will have external scrutiny of our draft policy, practice and procedure when those things are in place. We will also be able to take advice so that, when we finally deploy the devices, we can assure you and, importantly, the public that we are using the technology to keep them safe and doing so correctly.

Margaret Mitchell: I suggest that you perhaps do that before you formulate the policy, because that might be very helpful in getting the policy right in the first place.

Detective Superintendent Burnett: Thank you very much.

Stewart Stevenson: What I am hearing is that the kiosks extract no new information that you are not already extracting through the central processes. I can see that Detective Superintendent Burnett is nodding on that point. Therefore, you have a set of processes, procedures and rules, and you have registered with the Information Commissioner's Office your uses of the data in the central information system. The registration does not say what devices you do that on—I know that, because, like others, I am registered.

I very much welcome the existence of the vulnerable persons database—I am probably in it,

as a person of no concern. I do not want you to remove me from the database. I am not in it because I am a criminal or thought to be a criminal, but because I am connected to somebody who is vulnerable and you need to know about my connection. I am in the database so that you can contact me if the vulnerable person requires you to. Is that a proper description of a person of no concern? The label might be misleading about what is actually going on.

Detective Superintendent Burnett: Again, I apologise, but I am not proficient in the system. I do not use the system, so I would not like to answer at this point.

Stewart Stevenson: That is fine.

Daniel Johnson: You are saying that the kiosks do not provide genuinely new powers and that you have had the technology, in one form or another, since the 1990s. However, the amount of information that is contained on devices has exploded exponentially. Some information is of a sensitive and personal nature, and the information that is available now is not comparable to the data that was captured on SIM cards in the 1990s, which has been referred to. An officer having a look at what phone numbers somebody has on their SIM card is one thing, but giving officers the ability to look routinely at all the data that is now available requires additional sensitivity, because we are talking about a different category of information and level of intrusion. Do you acknowledge that difference?

Detective Superintendent Burnett: Absolutely. That is the challenge for Police Scotland and policing in a digital age. We need to be able to police in an age in which devices are commonplace in most of our inquiries, in some form or fashion. A device might be used in the commission of a crime or it might contain supporting information. The amount of information on devices is growing, but the public would expect us to have the right technologies to ensure that we can identify and utilise any pieces of evidence. It is right and proper for us to identify technologies to support us in our work in a digital age.

Your other point was about the access that police will have to sensitive data. That is nothing new for the police; it is part of being in the police. Unfortunately, a lot of the interaction that we have with members of the public is at the most traumatic times of their lives. On occasion in our inquiries, we need to take some really significant and intimate information and details. We interact with individuals at that time—that is part of the job of being a police officer, and we need to deal with it.

Rona Mackay (Strathkelvin and Bearsden) (SNP): I have a follow-up question to what my colleague, Daniel Johnson, asked about. Earlier, I think that you said that officers could put a filter in so that other personal information on devices would not be seen. Is that correct?

Detective Superintendent Burnett: That is absolutely correct.

Rona Mackay: Are you confident that that would always be done and that officers would not gather up personal data that they did not need?

Detective Superintendent Burnett: On the point that Mr Johnson made, because of the huge amount of data on a phone, the search parameters are there to make sure that, if we are looking for a text within a specific timeframe, we can do so. Can I guarantee that that will be done on every occasion? No, because the data that would potentially be pertinent to an inquiry depends on what is under investigation.

13:45

Rona Mackay: Were staff associations and unions consulted before the trials took place?

Detective Superintendent Burnett: I cannot speak to the time before the trials took place, but I can say that the cybercrime capability programme is one of the programmes of work as part of the policing 2026 strategy and the cyberinfrastructure project sits underneath that. We briefed the Scottish Police Federation and the police staff associations in autumn 2017 and gave them a demonstration of the kiosks.

Rona Mackay: Were any concerns raised by them?

Detective Superintendent Burnett: None whatsoever—they fully supported and saw the efficacy of the approach. They saw how it would support us to be more efficient in our processes and how it would support individuals, especially victims, by expediting criminal investigations.

Rona Mackay: I might have missed this, but are the trials still going on?

Detective Superintendent Burnett: No.

Rona Mackay: Has some form of formal evaluation been done? Will there be a report about what you have learned?

Detective Superintendent Burnett: A couple of brief reports were completed at the end of the trials and, prior to moving to the procurement of the kiosks, we liaised with a significant number of forces in England. As you will be aware, the kiosks are used by police forces throughout the UK and have been for a significant period of time. The reportage that came back was that we needed to make sure that our training, policy, practice and procedure were robust. However, the other

message that came through loud and clear was that, if we introduced the kiosks in the right environment, they would do nothing but assist us in giving a better service to the public.

Rona Mackay: Can you give us any feedback that you have received from the Scottish force so far on how the trials have gone?

Detective Superintendent Burnett: From what we have seen, the reporting was that submissions to the digital forensic hubs decreased dramatically. I cannot provide specific figures, but a dramatic decrease was reported, which meant that the investigation of crimes of significance in the hubs could be expedited. Basically, it let our specialist forensic examiners get on with the cases that really need that level of input.

Rona Mackay: Were no problems highlighted with the procedure and the practical side of it?

Detective Superintendent Burnett: None were highlighted.

The Convener: Superintendent Burnett, you talked about liaising with other forces around the UK. Was one of them North Yorkshire Police?

Detective Superintendent Burnett: I am aware of the report from North Yorkshire.

The Convener: Are you aware of the police and crime commissioner for North Yorkshire's report on the investigation into North Yorkshire Police?

Detective Superintendent Burnett: Yes.

The Convener: As I understand it, that report concluded, for instance, that there was a failure to receive authorisation for the use of phone extraction tools in half the cases sampled, and that poor training resulted in practices that undermined the prosecution of serious crimes such as murder and sexual offences. Were you aware of that?

Detective Superintendent Burnett: Yes.

The Convener: It also concluded that there were inadequate data security practices, including the failure to encrypt and the loss of files that might have contained intimate details of people who were never charged with a crime. Was any data lost as a result of the trials in Stirling and Edinburgh?

Detective Superintendent Burnett: No data was reported lost.

The Convener: You said that there were a couple of reports on the trials. Will you make those available to the committee?

Detective Superintendent Burnett: Yes, I will.

The Convener: Mr Hogg, can you say whether the Scottish Police Authority was sighted on either of the reports? If so, what was its response?

Kenneth Hogg: I do not know whether the reports were shared with the SPA, but I do know that, subsequently, a briefing was given by Police Scotland to the members of the authority in September 2017 in advance of the procurement exercise. That provided an opportunity for the members to ask questions about the proposed use of the kiosks and to seek the assurances that they wanted.

The Convener: Thank you. If a copy of that briefing or any presentation that was made could be made available to the committee, that would be helpful.

Liam McArthur (Orkney Islands) (LD): I apologise for my slightly late arrival. I was kept in the chamber for a debate that I was taking part in. I also apologise if some of what I ask about was covered in the exchanges that I missed at the start of the meeting.

Like Daniel Johnson and Ben Macpherson, I am slightly concerned about what appears to be a lack of preparation ahead of the trials. I accept the point about the perceived benefits of having the technology, which is already used but is being deployed further up the chain at the front line. DS Burnett said that the technology was nothing new and that the public would expect Police Scotland to deploy it. When it is moved closer to the front line, the extent to which it is used will grow exponentially and, therefore, the number of people who need the requisite training to be able to carry out the functions appropriately will expand if not exponentially then significantly.

I am slightly concerned that the deployment was not assumed to be a departure from what was already happening when it is, in the sense that it requires a good deal more officers to be cognisant of the sensitivities around handling the data. I would have thought that that should at least appear on a risk register.

Detective Superintendent Burnett: On officers being cognisant of issues to do with managing the data, prior to any use of a kiosk, they would still have the data. You have to remember that, if the device is of significance, it is put into the cybercrime hub, a download of the device is carried out and data is identified. Thereafter, that data is provided back to the inquiry officer for them to consider.

Liam McArthur: I am sorry to interrupt, but if you know that you will have to move the matter up the chain to the hub because that is the only way of being able to access the data, you will take a view of whether that is necessary as part of whatever inquiry you are undertaking. If, through one of the kiosks, you are able to identify that data there and then in the station, it will be far more attractive to do so. The cost benefit analysis that

you will do about that will be very different from what it has been traditionally when the device has been sent to the hub. Therefore, having the kiosks in place will result in an increased usage. The technology will be used in instances in which it is not used at present.

Kenneth Hogg: Through the SPA's involvement in oversight of the procurement of the cyberkiosk devices, I can tell you that the procurement included a training package. Included in the cost that I mentioned earlier was a sum of money to train trainers in Police Scotland in recognition of the point that you make. If we have more people operating devices, they all need to be trained appropriately in using them. Therefore, that has been taken into account.

The other key point that links to that is that, at the moment, devices are sent to the hubs, where there is a less discriminating download of the data. The so-called kiosks allow for more parameters to be set. Therefore, for the first time, devices are being examined using a narrower set of search parameters than currently happens when the devices are sent out.

Liam McArthur: In relation to any decision on wider roll-out, what further safeguards are being considered on data protection or human rights issues? There is a gamut of issues that, I presume, has come up already because the technology is being used in other areas. However, if it is being used more extensively by a wider range of people in Police Scotland, another analysis will have to be done to ensure that the safeguards remain appropriate.

Kenneth Hogg: That is where the importance of the standard operating procedure, to which DS Burnett referred, comes in. It is intended that, before it is developed, the procedure to be established on the devices' use will be given to the external expert reference group for consultation, so that concerns or questions about privacy, data, usage and consistency can be built in.

As matters stand, there is not an agreement to roll out the devices. Roll-out will not happen until the issues that you have raised are addressed, including through that external expert group.

Liam McArthur: Is the external expert group self-contained or will it receive submissions? We have received a number of submissions in advance of today's meeting. Will the group invite the organisations that have been in touch with us, and perhaps others, to submit their views ahead of any decisions that it takes?

Kenneth Hogg: Yes. I understand that Police Scotland intends to invite Privacy International to be a member of the group.

Liam McArthur: Is it the case that, at this stage, there is no ballpark timeframe for roll-out?

Kenneth Hogg: There is a plan. As I have mentioned, this work comprises part of the implementation of the policing 2026 strategy. The intention is to engage with the group over the summer and to work up the standard operating procedure in order to allow roll-out in the autumn. That is not the same as saying that there is agreement at this stage to proceed with roll-out; agreement would follow only once the group has done its work and the procedure has been put in place.

Daniel Johnson: Before I ask a technical question, I want to ask about how the work fits in with the information technology strategy, given that the strategy has not yet been signed off. Could you get back to us in writing with the details of the IT strategy and how the procurement fits in with it? That would be useful.

It is unfortunate that the figures that you have cited are exclusive of VAT, given that Police Scotland cannot recover VAT. I ask that you make sure that that does not happen again when you provide information.

Kenneth Hogg: I am sorry. I was quoting figures—

Daniel Johnson: The VAT position has changed, so my basic point is that citing VAT and ex-VAT numbers is confusing.

On a technical point, my understanding is that some phones, if users set them up correctly, have sophisticated data encryption levels, which even the Federal Bureau of Investigation cannot crack. My phone is set to "Data protection is enabled". I guess that means that the kiosks would not work on my phone. Am I right in saying that encryption means that the kiosks would not be able to find anything on such phones, or is that incorrect?

Detective Superintendent Burnett: As you have alluded to, technology changes all the time, as do the devices. Different people have different devices that have different security set-ups. Some devices are set up with security. If we are able to plug those devices into the kiosk, we will be able to access the data on them. The list of those devices changes all the time in terms of how technology is—

Daniel Johnson: But all Apple iPhones and Android-based phones, which comprise the vast majority of smartphones, have, as part of their operating systems, the ability to encrypt all data. I am assuming that savvy serious organised criminals know all about that. I am guessing that the kiosk gets those people who are less savvy and more occasional—

The Convener: Daniel, I do not think that we necessarily need to go into that. Police Scotland will be able to extract data—

Daniel Johnson: Will it be able to extract data from an encrypted phone?

Stewart Stevenson: Yes.

The Convener: Yes. I beg your pardon, Detective Superintendent Burnett—by all means, answer the question, if you wish.

Detective Superintendent Burnett: Kiosks are part of a suite of options that are available to Police Scotland and UK law enforcement. You have alluded to the fact that, as every law enforcement agency is, we are challenged by policing in a digital age. That is something that we have to consider.

14:00

Ben Macpherson: You mentioned that no data is retained on the kiosks and you answered a question from the convener about data loss. Do the kiosks have any capability to delete information that is on devices?

Detective Superintendent Burnett: Not as far as I am aware.

Ben Macpherson: It would be good to get clarity on that.

Detective Superintendent Burnett: Absolutely.

The Convener: It was certainly the view of the investigation by the police and crime commissioner for North Yorkshire that that was a possible consequence.

Detective Superintendent Burnett: I will get confirmation of that, convener.

Ben Macpherson: It would have different consequences if that were possible.

Detective Superintendent Burnett: Clearly.

Stewart Stevenson: Convener, I think that the commissioner was making a point about data on the kiosk, whereas I think that Ben Macpherson was asking about data on the device. They were different points.

The Convener: Okay. I can see that it is a very technical matter.

I have a few questions for you, Detective Superintendent Burnett. What discussions has Police Scotland had with the Crown Office and the Lord Advocate about its use of the equipment?

Detective Superintendent Burnett: Back in 2016, prior to commencement of testing of the devices, the Crown Office was consulted. The purpose of us using kiosks is to secure any evidence that can expedite a criminal investigation, so there is no point in us considering it in isolation. We need to know that the Crown Office is supportive of, and comfortable with, use of the kiosks and the seizure of evidence in that way. It was supportive of the trials but said at the time that, because it was a new use of the technology, it would support its use only in summary cases, but we have—

The Convener: Summary cases.

Detective Superintendent Burnett: Yes, summary cases. That was during the trials. We have continued in consultation with the Crown Office since then. It is aware of our procurement and is supportive of the use of kiosks within the lawful framework that we discussed earlier.

The Convener: Okay. Would you be able to share that correspondence with the committee?

Detective Superintendent Burnett: Absolutely.

The Convener: As I understand it, in Scots law, a person can be a witness, a suspect or an accused—I think that you alluded to those statuses, detective superintendent. Do people in any of those groups have the right to say that the police are not getting their phone? You talked about interrogation. We all understand the issues in cases that involve domestic violence, vulnerable persons or missing persons, or in which there is a pressing need because life is threatened. Will you write to us about who can and cannot refuse to hand over their phone?

Detective Superintendent Burnett: Of course. Are you talking about providing the device?

The Convener: Yes.

Detective Superintendent Burnett: Clearly, a witness could refuse to provide a device to expedite any inquiry. For a suspect or an accused, a phone would need to be seized under a lawful purpose—one of the ones that I discussed earlier.

The Convener: Police Scotland's submission is not in plain English. I had difficulty with the phrase:

"the design principles underpinning our planning emphasise an approach which will be modular, iterative and agile".

I am an old-fashioned bloke and that does not make much sense to me. However, what jumped out at me was the mention of undertaking

"an Equality and Human Rights Impact Assessment and Privacy Impact Assessment before operational deployment."

We have covered the fact that your trial was not supported by any of those documents. Are you not putting the cart before the horse? What if that human rights impact assessment said that there were implications? We have already had the expenditure of £1 million.

Detective Superintendent Burnett: Convener, because we use the technology anyway and are aware of its use and efficacy throughout UK law enforcement, we absolutely understand the need and requirements. We are completing those assessments and will build in any findings from them. I do not anticipate that anything will come up in those assessments that we cannot address. Clearly, if there is anything that means that we have to stop the deployment, that would need to occur.

The Convener: There were opportunities to reassure us fully on the matter. Personally, I am not reassured and I understand that others might not be, either. We will discuss the matter as part of our work programme and might well come back to you in writing. In the interim, it would be helpful if you could send the committee the papers that we requested. I thank you both for your evidence.

Detective Superintendent Burnett: Thank you, convener.

The Convener: We now move into private.

14:05

Meeting continued in private until 14:18.

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