OFFICIAL REPORT
AITHISG OIFIGEIL

Justice Sub-Committee on Policing

Thursday 15 November 2018

Session 5

The Scottish Parliament
Pàrlamaid na h-Alba

Thursday 15 November 2018

CONTENTS

JUSTICE SUB-COMMITTEE ON POLICING
12th 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:

Clare Connelly (Faculty of Advocates)
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 15 November 2018

[The Convener opened the meeting at 13:00]

Digital Device Triage Systems

The Convener (John Finnie): Feasgar math, a h-uile duine, agus fàilte. Welcome to the 12th meeting in 2018 of the Justice Sub-Committee on Policing. We have apologies from Daniel Johnson. The only item on our agenda today is an evidence session on Police Scotland's proposed use of digital device triage systems, which are more commonly referred to as cyberkiosks.

I welcome Diego Quiroz, policy officer, Scottish Human Rights Commission; Detective Chief Superintendent Gerry McLean, head of organised crime and counter-terrorism, Police Scotland; David Freeland, senior policy officer, United Kingdom Information Commissioner's Office; and Clare Connelly, advocate, Faculty of Advocates. I thank the witnesses for their written submissions, which were helpful.

The sub-committee first considered this matter on 10 May, and this is the fourth occasion on which we have considered it. The initial questions were all around the legal basis on which the use of cyberkiosks would take place. I am somewhat surprised and disappointed that we do not have something definitive in front of us regarding the legal position that Police Scotland believes supports its deployment of the devices. Can you update us on that, Mr McLean?

Detective Chief Superintendent Gerry McLean (Police Scotland): Thank you for inviting me to give evidence today. When I last gave evidence to the sub-committee, a number of substantive points were raised, one of which was around establishing a legal basis for the use of the device. Obviously, we are confident of the legal basis on which Police Scotland applies the law in relation to digital forensics at this time. I tried to give that assurance to the sub-committee the last time that I appeared before you. Since that date, our chief officer who is the senior responsible officer for the cyber programme, which involves cyberkiosks, has written to the Crown Office, and we are taking legal advice from our legal services department. We still await a response from the Crown Office. I spoke with its representatives as recently as yesterday. My understanding is that the issue is being considered at a senior official level in the Crown Office, across its policy division, its cybercrime division and its serious crime unit.

Our legal services team supports the position that I articulated to the sub-committee previously. I hope that I described the extent of the powers to you then, but I accept that, across some of the document sets that go to the sub-committee and others, we have to be clear about how we articulate that.

When we search, seize and retain devices under a warrant, power is conferred by the court and under some statutory provisions—I think that I have previously provided examples to the sub-committee of the legislation that is available to us in that regard, such as the Firearms Act 1968 and the Misuse of Drugs Act 1971. More particularly, advice was given to us that it is important to make distinctions to all concerned between victims and witnesses, and to be clear about the circumstances in which there is no compulsion on the part of individuals to hand over their devices—that must be done on a voluntary basis.

We have some powers that were enacted by this Parliament in the Criminal Justice (Scotland) Act 2016, which allows for arrested persons under that legislation—suspects or accused—to be searched and for any items that are in their possession at that time to be seized. That is the statutory provision that underpins some of the other statutory courses of action that are open to us where powers are not conferred on us by the court through a warrant.

The Convener: The Lord Advocate is in charge of investigation of crime in Scotland, and Police Scotland undertakes that on behalf of the Lord Advocate. Therefore, is it not somewhat surprising that, given that everyone wants to facilitate the thorough investigation of crime, there is not something as simple as a letter before us to confirm your understanding of the position? People will make the clear distinction between you having the statutory authority to investigate cases under the legislation that you have mentioned and the common law, on one hand, and, on the other hand, situations involving complainers and witnesses, which is where most of the concerns lie.

Given that the sub-committee commenced this process on 10 May, are you not surprised that the Parliament has nothing to confirm that the Crown Office and Procurator Fiscal Service supports your position?

Detective Chief Superintendent McLean: I recognise the sub-committee's frustration about that. The position might well be described as not being a binary position about whether there is legislation or not—Scottish law is based on a number of often competing principles. I have

previously tried to describe to the sub-committee some of the statutory provisions that are allowed to the police and some of the powers that are conferred through warrants, as well as the competing demands and how we try to apply the law that is available to us at this time. It is a complex issue and some of it is examined in the courts through case law. That has been referred to previously at the sub-committee, and that is what supports the legal basis on which we think we are empowered to undertake digital forensics and thereby the potential roll-out of kiosks in the future.

The Convener: Have you had individual discussions? Have you discussed matters with the Crown Office, Mr McLean?

Detective Chief Superintendent McLean: We have not had those discussions. We have just had follow-up discussions about when we may get some direction or response from the Crown Office.

The Convener: What was the answer to that?

Detective Chief Superintendent McLean: It is under consideration.

Diego Quiroz (Scottish Human Rights Commission): I hope that the sub-committee is not tired of hearing from me. Thank you for inviting us to give evidence. I totally agree that it is a complex issue, and that is why we are asking for clarity. There is a need for clarity and it is important to state from the beginning that the lawfulness of the technique is highly fact dependent. However, we can say that there is no legal basis outside the context of a warrant, and that is because it entails a significant interference with rights under article 8 of the European convention on human rights, which is not accompanied by the required legal certainty and adequate safeguards against abuse and arbitrariness. It is important to acknowledge that. The legal basis for the techniques argued by the police appears to be founded on a number of contexts and statutory provisions arising in many different circumstances. That makes their legality highly fact dependent, and it seems quite reasonable to say that we therefore do not have a legal basis for such examinations of mobile phones.

The Convener: Ms Connelly, would you care to comment?

Clare Connelly (Faculty of Advocates): I, too, have some sympathy with Police Scotland and the Crown Office in trying to present to you a robust legal framework that legitimises what is proposed. We are not the first jurisdiction to face this problem. In 2013, Mr Justice Cromwell, a Canadian Supreme Court judge, highlighted that the traditional legal framework that would surround search of individuals and their property requires updating in order to protect the unique privacy interests that are at stake in computer searches. The reason for that is that searching a computer—smartphones are computers—is not the same as searching a cupboard or a filing cabinet. A warrant that is granted to allow an office to be searched can set very strict parameters. When you access a person's mobile phone, you do not access only what is contained in the device in your hand; it is a gateway to the cloud and to external sources of information.

The fact that Police Scotland representatives have returned a number of times without the clear legal framework that you are looking for reflects the complexity of that challenge. So far in case law, we have seen that, when it comes to examining mobile devices, the Scottish courts rely on the traditional legal approach. In my respectful submission, that traditional legal approach is not fit for purpose, and that is a matter that needs to be looked at again.

Stewart Stevenson (Banffshire and Buchan Coast) (SNP): I wonder whether the complexities might be susceptible to trying to granularise the issue. I want to do that in a particular way.

Is there a different set of law that applies to the seizing of a phone as opposed to the subsequent searching? I can see—this is not a legal statement—that it makes logical sense to seize a phone to protect it because it would be interfered with in some circumstances, even if there might have to be a legal process to allow the searching of that phone, just as the police might secure premises but not have the right to enter and search them. Is it reasonable to look at the problem not as a single problem but as a sequence of different legal competences or questions that need to be asked? I think that "Seizing" and "Searching" sound like two useful headings. Am I right or wrong in looking at the matter in that way?

Clare Connelly: That is a reasonable approach. Underpinning both is the fact that we are dealing with current technology, and the legal regulation of that involves the application of laws that could not have envisaged when they were developed that we would have that level of technology.

Another difficulty is that those who make determinations about the admissibility of evidence are old people like me who use their phone to telephone people and, perhaps at a push, manage to send a text.

Stewart Stevenson: Age is relative, of course.

Clare Connelly: That is as opposed to my teenage children, who use those devices in a very different way. If you asked someone whose mobile phone use reflects mine, they would say that there is probably not that much of an invasion of privacy compared with doing other things that have always

been done. However, there is a huge generational gap in how the devices are used, so there is a difficulty in assuming that there is safety around the investigation of them because they do not hold much information.

Liam McArthur (Orkney Islands) (LD): I want to pick up on Ms Connelly's and Mr Quiroz's responses. We have entered into a debate about kiosks, but it strikes me that what we are discussing could equally apply to what has happened traditionally in the hubs. Is that a fair assumption?

Clare Connelly: That is slightly different. For example, when a computer tower is taken to a hub, the tower is not switched on. The hard drive of the tower is imaged, and there is then an interrogation and search around that image. That allows people to search only what is contained within the memory of the tower. At no point would a person switch on the computer, because there is an interference process.

In my respectful submission, one of the difficulties with the kiosks is that they turn the phones on, so there is a gateway to what is stored on the SIM or an equivalent memory device in the electronic mobile phone or whatever it is, and a person could access the web and externally stored data in a way that they could not from the imaging of a computer tower. Having seen the difficulties that arise from that process in a fraud trial, I know very well that, when the imaging was done and we were given it, we had to ask what to do with it, because programs have to be used to be able to read the image.

Liam McArthur: But I presume—

The Convener: I saw Mr McLean shaking his head about some aspects. Maybe it would help to clarify them.

Detective Chief Superintendent McLean: It might be helpful to the sub-committee and others to consider some points of accuracy on that. I will try not to take too much time.

I go back to Mr Stevenson's point about whether there is a bespoke piece of legislation that covers that eventuality. I think that we are saying collectively that there is an absence of that. That is why I said that the landscape is complex, but there is a set of principles. I refer to the Criminal Justice (Scotland) Act 2016, which covers most eventualities for an arrested person, and it gives the power to search and to seize. When we start to question that, we question seizing any material and the power to examine it.

On my esteemed colleague's point about a filing cabinet or storage, as a point of accuracy, when a kiosk examines a device, that device will be switched off. If it has a SIM card, it will be removed. It will only be stored data, which brings it very much in line with the case law that looked at stored data on devices and found that the police acted correctly when using those powers to search devices. I accept the point about the devices that a modern society will bring.

13:15

We talked about the article 8 implications. The police work with those in mind every day, along with the other ECHR articles—in particular, on the right to life. Without getting into a legal debate, it is important to note that the article 8 rights are not absolute. The rule and administration of law are important and they can be exceptions to the article 8 rights. With powers that are conferred by a warrant or statutory provision, we can take consideration of article 8 for persons who have been arrested, but they are not absolute rights.

Liam McArthur: Mr Freeland and Mr Quiroz were both nodding in agreement. Does the issue around the legal basis extend beyond the functioning of the kiosk process?

Diego Quiroz: Absolutely. It is even more serious and significant in terms of interference when it comes to the hubs, because there are issues with data extraction, retention and management. There is the matter of the right to privacy, but there are also data protection laws. I certainly agree with you.

Liam McArthur: From conversations with the Crown Office, is the expectation that what will come back by way of a formal response will capture what Mr Quiroz just indicated in relation to the legal basis for the hub process, as well as the kiosk process?

Detective Chief Superintendent McLean: With respect, I would not presume to speak on behalf of the Crown Office, but that is a valid point. I support what Mr Quiroz said. The intention with the introduction of cyberkiosks is to introduce a triage process to stop so many devices going to the cyberhubs. The legal basis for both those systems is the laws that I previously described.

David Freeland (Information Commissioner's Office): I absolutely agree. If more devices are filtered out, there is less privacy intrusion. However, that does not get away from some of the data protection risks that are inherent in the cyberhubs due to the volume of data and questions over the relevance of the data that is processed in them. As I said to the sub-committee previously, we are looking into that question as part of our investigation into such technology throughout the UK. Colleagues have given evidence in Westminster on our concern about the volume and relevance of the information that the

police are processing from modern smartphones and mobile devices.

Margaret Mitchell (Central Scotland) (Con): Mr McLean, are you saying that you think that the existing case law is sufficient to back Police Scotland's powers to seize a phone and to look at and process data from a seized phone?

Detective Chief Superintendent McLean: I was asked before at the sub-committee whether I felt that there was a legal basis for searching and seizing devices and whether I would keep that under consideration. From the legal advice that we have taken internally—we will not presume to know what the Crown Office would tell us—we are satisfied that, from the powers that I have described, there is a legal basis for us to search and seize those items.

There is a general agreement among colleagues who have supported some of the reference groups that a modern society should always keep its laws under review; we should accept that. There are a number of complex issues that the police have to manage within that legal basis, but we are satisfied at this time that the legal basis has been tested in the criminal justice system.

Margaret Mitchell: In that case, do you see no difficulty at present in passing the legal tests of foreseeability and accessibility?

Detective Chief Superintendent McLean: Yes. However, we have to be more explicit. I accept from colleagues in the various groups and from the consultations that we have done that we might have been ambiguous about what the powers are. In terms of the clarity of the law, we need to be more explicit about what the powers are and who they are applicable to, so that it is foreseeable to people what they can expect the law to be able to do to them and what rights they have. It is about the distinction between a victim or witness and a suspect or accused, and what powers are available to the police.

Margaret Mitchell: Whatever the situation is, if there is ambiguity, I suggest that there is not the necessary clarity in the law that is essential on this issue.

Detective Chief Superintendent McLean: I think that there is a question about the clarity of the law, but I still think that there is a legal basis to search and seize devices.

Margaret Mitchell: To search all the data? I will bring Mr Quiroz in here, because I think that the Scottish Human Rights Commission has doubts about that and considers that there should be, for example, independent oversight of the use of mobile phone browsing.

Diego Quiroz: Absolutely. As I think we are all saying, it is an incredibly complex framework, which applies in different circumstances. It is therefore difficult, if not impossible, to discern the legal powers that the police have to use that technique by just applying logic, as was said. There is a lack of specificity in the current law, which is something that we think is required in the framework.

The point about the seizure of evidence from a human rights perspective is that the powers that traditionally allow the police to seize items cannot be considered and applied in the case of mobile phones. There are no separate powers for the examination of seized items and most of the provisions that were referred to are parasitic on other powers. That means that they have different meanings and different purposes. That seems to be all merged into one single legal basis for the use of cyberkiosks.

The differences are particularly clear when we are talking about electronic devices, which goes back to the point about the Canadian Supreme Court and US Supreme Court cases. They clearly state that searches and examinations of mobile phones should be done within the legal framework of a warrant. In the case of Canada, there are only very narrow circumstances in which those searches can be done without a warrant and it depends on the criminal offence and the immediacy of the circumstances. Certainly, the Canadian Supreme Court is quite clear that minor offences will not allow the use of mobile extraction or browsing without a warrant.

Margaret Mitchell: Do the other witnesses think that the legal basis is sufficient? In particular, Mr Freeland, it has been suggested that the roll-out should be postponed; the European Court of Human Rights has suggested that because of its concerns. I know that the ICO says that there should be no roll-out before the data protection impact assessment and other documents are in place.

David Freeland: We have now seen a copy of the data protection impact assessment and have provided substantive comment back to Police Scotland on a number of the issues. Mr McLean has taken that on board and we hope that we will have a revised version on that basis. One of the questions was about the legal basis, because it was not sufficiently clear to us what that basis was. I am not an expert in criminal law, so we need Police Scotland to spell out for us what the basis is in this case. Until that is there, we cannot be clear that the practice in question is lawful. Data protection law says that the processing of personal data needs to be lawful. If we cannot clearly evidence that, I question whether that processing can go ahead.

I am not an expert in human rights law either, but I note that the European Union law enforcement directive, which sets out the rules for processing personal data for law enforcement purposes, states in its recitals, or reiterates, that member state law must be precise and "accessible, clear, foreseeable" and must be in compliance with the rulings of the EU courts and the European Court of Human Rights.

Clare Connelly: The 2016 act certainly empowers police officers to stop and search, but that does not necessarily give the article 8 protections that are clearly of concern to the panel and to you. For that reason, I would say that we do not have a fit for purpose legal framework in place at the moment to allow the roll-out of the policy and the use of cyberkiosks without interfering with the article 8 rights of individuals.

Margaret Mitchell: Is the December roll-out date looking very suspect, especially from the human rights perspective and the perspective of the commissioner because of the data protection impact assessment and other documents that have still to be received?

David Freeland: We need clarity on a number of the key issues that we have all identified to Police Scotland. We should not necessarily be putting dates on it; it is more that resolving the issues will be the gateway to roll-out.

Margaret Mitchell: Mr McLean, is there a possibility that the issues can be resolved by December? I would have thought that that was a very tall order.

Detective Chief Superintendent McLean: I would rather say that it is very ambitious, but perhaps that stretches the level of my ambition. Police Scotland is being as transparent as it can be and is consulting a range of partners as best it can. We are extremely grateful for the contributions that they have made to the considerations that we clearly have to make ahead of any planned roll-out of cyberkiosks.

There are still substantive issues. A key thing is the clarity in how we have positioned or articulated the policy. In short, there is an opportunity to get this right, but we have to take a measured approach in order to do that to the best of our ability in a very complex legal landscape.

I probably concur with your view that December is very ambitious; there is still more work to be done. Police Scotland's position is not that we should roll out the kiosks at any cost. It is about getting all the document sets and allaying the concerns of the people of Scotland and the people who have engaged with the stakeholder and reference groups.

Margaret Mitchell: To put it another way, rather than there being a need to get it right, there will be dire consequences if you get it wrong, which would jeopardise the whole project. Perhaps it needs a little less haste, to make sure that the authority to seize items and look at the data is absolutely tight.

Rona Mackay (Strathkelvin and Bearsden) (SNP): My question is for Ms Connelly, but it probably applies to everyone. You were talking about how an old legal framework is being applied to new technology. In your opinion, does it need new, or amended, legislation?

Clare Connelly: It probably does. I do not think that it is possible or reasonable to expect the existing common-law case law to be developed in court process for an issue as important as this, which has been flagged up in advance.

Rona Mackay: That is interesting.

Diego Quiroz: Absolutely. The point here is to provide Police Scotland and the police in other authorities with an adequate framework so that they can do their important work. As I said last time, it is very much about protecting our human rights in a way that does not interfere with that job.

There are significant issues in terms of lawfulness. Legal certainty, foreseeability and safeguards, which the convener touched on, are not adequately provided in the current framework. There is a need to provide such a framework to the police, and the Parliament and Government are the source of that.

13:30

The Investigatory Powers Act 2016 has a similar context. The UK Parliament looked at communications interference and personal data-related issues, and it looked at all the legislation and said that it was not enough. It said that it was unlikely that common law could be considered as a legal basis and that a framework needed to be developed. It developed a quite comprehensive framework through the Investigatory Powers Act 2016, which is not perfect—it has been challenged a couple of times, even in the Supreme Court—but it gives legal certainty and provides enough safeguards.

As members probably know, there is the Investigatory Powers Commissioner's Office. The UK Parliament's Intelligence and Security Committee has oversight of the legislation, and there are the Investigatory Powers Tribunal and four or five codes of practice. The legislation has also incorporated the Wilson doctrine and the protection of journalists, doctors and lawyers so that personal data does not flow everywhere. As

members know, a judge who serves in the IPCO reviews the warrants.

That illustrates what is happening and how the UK Parliament has reacted to the challenges of modern technology to provide the police with adequate tools to do their job.

Rona Mackay: I have a question for Mr McLean. I know that we have covered assessments quite a bit in previous sessions. I do not know how honest you can be about this but, in hindsight, was Police Scotland a bit premature and did it jump the gun in having the roll-out without having considered all the issues? I know that that comes down to assessments.

Detective Chief Superintendent McLean: It was alluded to earlier that the cyberkiosks issue has opened up a much wider discussion about the complex landscape that the police are trying to operate within. The ambition and sentiment behind cyberkiosks was to have better service delivery and to minimise intrusion. A much wider discussion about that has been caused.

My personal view is that even our view of impact assessments at the very start of the journey would still not have been sufficient for where we currently are. We are learning every day on the job, and the contributions that people around this table and other contributors to the reference groups make enrich the discussion and our considerations about the wider privacy safeguards. We are on a journey.

Stewart Stevenson: Given that the kiosks are essentially doing the same investigatory task as the hubs in a broad sense, does this discussion apply equally to the hubs?

David Freeland: As I said before, cyberkiosks have brought matters to public light and are one part in the chain of how evidence is obtained in criminal cases. If we look along that chain, we see that there are questions in other parts of it, including about cyberhubs.

Liam McArthur: I want to follow on from Rona Mackay's line of questioning. I appreciate Mr McLean's candour in a number of sessions, and it is only fair to put on record a statement by the Open Rights Group in its submission. It said:

"Open Rights Group welcomes the openness and engagement in the consultation process that Police Scotland have undertaken."

Notwithstanding the seriousness of the concerns, the approach that Police Scotland has taken since those concerns came to light has been encouraging.

Ms Connelly and Mr Quiroz referred to legislative change. Should the Scottish Law Commission look at that? There is always a risk in leaping to pull the legislative levers that we end up putting in place something that is fairly rigid. When we are dealing with technology that is advancing in the way that it is, we might find that we are already behind the 8-ball again by the time the legislative process is completed. Is this something that we should be inviting the Scottish Law Commission to consider or does it require a more streamlined legislative fix?

Clare Connelly: It is not at all straightforward; it is a Pandora's box. It is particularly complex, not only because of the legal aspects of making such interrogations legal and compliant with the convention but because we are trying to keep up with the rapidly expanding body of technological processes—it is ahead and we are running behind. Therefore, fully researched considerations of all possible manifestations of future technological developments by a body such as the Law Commission would at least allow the possibility that the legislation could have some longevity, rather than—as Mr McArthur says—be out of date by the time it is on the statute book.

Liam McArthur: That takes us into a whole different ball game. Mr McLean was fair to say that a December roll-out is fairly ambitious. If we go down the route that you suggest, the roll-out might be in December but we might have to pick the year.

Clare Connelly: Absolutely. As many people have said, the cyberkiosks have highlighted a much broader issue, including the use of dashcams in criminal prosecutions and the use of the cyberhub. That is the quandary. It is something that needs to be carefully considered, but time is of the essence. We are up against it, both to ensure that current practices are compliant with our convention responsibilities and to ensure that we do not have further infringement of people's rights, for example by the use of dashcam evidence, which raises similar issues.

Liam McArthur: Are you suggesting that care and attention need to be applied to what is currently being done—there might need to be a review—and that the rolling out of cyberkiosks would not be sensible until that legal framework is in place?

Clare Connelly: That is correct. There is currently reliance on evidence before the courts that interferes with the article 6 and article 8 rights of the individuals involved and that is of grave concern. What is needed is an expert group to work intensively to consider the matter quickly and in depth, prior to commencing a legislative process.

Liam McArthur: Are there any other views on that?

Diego Quiroz: That is a different question from the question of the legality of the cyberkiosks and the particular technical approaches that we are discussing. It is up to the Parliament and the Government to decide which path to take. There are several issues that are nominally related to cyberkiosks, such as the use of cameras, computers and other devices, so there could be a broad, comprehensive piece of legislation to cover all forensic digital media. Another path to go down might be to develop a code of practice for the specific issue, which could be laid before Parliament for scrutiny. There are different paths that you could take, but it is important that the Parliament keeps oversight of the process, as it has done so far.

Detective Chief Superintendent McLean: I do not disagree with anything that has been said. However, it is important to say that, as a police force, we only apply the law that is provided to us.

I said earlier that Scots law is essentially a set of principles, and a change that is made in one area can adjust the relationship between those principles. We have to consider the unintended consequences of any decision on cyberkiosks not only for wider digital forensics but for other parts of the criminal justice system. If cyberkiosks are adopted and supported by way of review, the principles that are applied to them will be interpreted in other criminal investigations and prosecutions. We have to be cautious here and, as Diego Quiroz has said, consider every option.

Liam McArthur: Can you give us an example of an obvious read-across in the criminal justice system?

Detective Chief Superintendent McLean: We could say that, given the potential for infringements with and the lack of safeguards for cyberkiosks, we will stop all digital forensics. However, most cases that go in front of a court or into the criminal justice system describe our lives in some way, and those lives are surrounded by digital devices. That is a consideration.

We also need to consider article 2 and the right to life. In high-risk situations such as those involving missing persons or crimes in action, stopping digital forensics would denude us of that capability and leave us unable to respond—or, at least, would limit our response with regard to some of our article 2 obligations.

However, the issue might well go wider than digital forensics. Where do you draw the line with sensitive or personal information, which might not come just in a digital format? Adopting a set of principles for one part of the criminal justice system might have unintended consequences elsewhere.

The Convener: I should say that we are looking at this matter not because of the hubs but because a different approach is being taken and we need to understand the wider implications.

I want to ask two or three specific questions. I think that you said that the cyberkiosks do not turn phones on, but at a previous meeting, Mr Quiroz said that they can access texts, photos, web-browsing history and biometric data such as the fingerprint that is used to turn a phone on. Is that correct?

Detective Chief Superintendent McLean: It might be. What happens is that the mobile device in question—let us call it a phone—is switched off and the SIM card removed, which means that it does not connect to any external source of information through a network, wi-fi or the internet. The cyberkiosk then provides some search parameters that allow us to ask a series of questions about the data that is stored on the device, be it a phone or whatever.

The Convener: That sounds like the answer is yes, and that the information—for instance, web-browsing history—can be accessed.

Detective Chief Superintendent McLean: It might be possible; it depends on the device. It is not that I am not taking a position on this—it just depends very much on the technology that is plugged into the kiosk. However, what you suggest is possible.

The Convener: Would that include the fingerprint that is used to activate the phone?

Detective Chief Superintendent McLean: When that specific question was asked—indeed, I think that Mr Quiroz was present at the time—it was said that it was extremely unlikely that it would have that capability. We can say with some confidence that it would not do that.

Diego Quiroz: It is a technical question, and the explanation that we got is quite interesting. The fingerprint that unlocks a phone is not actually a picture of a fingerprint but a mathematical formula that describes it. I asked the same question when I spoke to the police, and I was told that it would be very difficult to match that formula to an actual fingerprint. The transition from the call-in of a picture to the actual picture is a complex process. Is that not correct?

Stewart Stevenson: I might be able to help here.

The Convener: I think that Mr Stevenson is going to tell us what he knows.

Stewart Stevenson: Just as banks do not need to know—and, indeed, do not know—your personal identification number to validate that you have put the right one in, there is a one-way

algorithm in phones and so on that takes the image and produces an answer from which you cannot derive the original data. That process is repeated every time the data is offered, so you cannot take the data and work out where it has come from. If you want the technical explanation, it is what is called a one-way algorithm using a matrix transformation corner to corner.

The Convener: Aye, we all knew that. [*Laughter*.]

Diego Quiroz: Thank you for the enlightenment, but it does not make the process any less intrusive. There is other biometric data that can be downloaded such as an individual's voice, his or her pictures and other incredibly personal material about his or her personal relations, his or her identity and even third parties.

13:45

The Convener: I will try an example, Mr McLean. Forgive me: we have run this example before, but I want to understand. The notion of consent is an easier concept for me. An accused person and a suspect will have a measure of protection. If a complainer said that they had been sent an offensive image and presented themselves at a police station that had a cyberkiosk, would it be used to establish whether there was an indecent image? In the process of doing so, would it be able to look beyond? If the person said that someone had sent them an offensive image within the past hour, would the parameters of the search be limited to that timeframe?

Detective Chief Superintendent McLean: The straightforward answer to that is yes. That is the whole intention of the kiosks. It is a triage process. As you know, the thin blue line is very stretched. Officers want to ask the question and get the answer. The whole intention behind the kiosks is to eliminate a device at an early stage if possible and to return it to its owner, thereby providing a much better service not only to the investigation at the front end but to the public and the owner of the device, whether they are a witness, a victim, an accused or a suspect. The intention is to get the devices off our shelves and back into the hands of their owners.

To answer your question more specifically, the kiosk allows people to ask the specific question: was an offensive image, a text message or whatever is under investigation delivered in a time parameter between specific dates? The kiosk will throw up results, but its capability in terms of looking through the whole catalogue of images and data on the device is limited—as is that of officers. The intention is to interrogate the phone by asking it a series of questions via the kiosk.

The Convener: The wider concern about the employment of the kiosks might be that the police could go on a fishing expedition.

Detective Chief Superintendent McLean: Yes, I have heard that position being put. As I have said, we are putting checks, balances and safeguards in the training programme for the operators. The device will not be interrogated by an investigator who has a desire to try to prove the case and who might be unduly influenced. The safeguards involve supervisory checks of the operators and will consider many of the things that need to be thought about, such as proportionality, necessity, collateral intrusion and understanding the matter that is being investigated and what the investigating officer wants to try to get from the device. Those separate officers will interrogate the device and come back with results for the investigating officer. We have put in checks and balances in that regard.

Clare Connelly: My concern remains that search parameters will be put in, but in many cases that one could anticipate, the search cannot be targeted at the single thing that is being looked for. Although a fishing exercise might not be carried out, the way in which the law operates means that, if police officers come across incriminating material in the course of a search, even if it is outwith the limits of a search warrant, for example, it becomes admissible. Therefore, although a fishing exercise is not, strictly speaking, allowed in law, if officers come across incriminating material by accident or in the process of carrying out a search, that is deemed to be admissible evidence.

The Convener: On that particular example, Mr McLean, if someone received two images that might be deemed to be indecent and they are unhappy with the sender of one but are not bothered about the other image, could that turn a complainer into an accused?

Detective Chief Superintendent McLean: I suppose that I cannot judge every eventuality. The point is about self-incrimination, but I sense that your example is probably less to do with an accused person and more to do with a victim or a witness. We cannot compel victims or witnesses to give over digital devices for examination; there has to be a voluntary element. The quality of the law and the other things that we have talked about need to be considered. We need to be more explicit about what we mean and what the expectations are.

If a police officer comes across something in the searching process that indicates other criminality, perhaps of a grave nature, it is clear that they would have some responsibility. That is true of many searches—a search of a filing cabinet, for example, let alone a search of a digital device. At

that point, it becomes extremely complex. Do the powers that are being utilised at the time empower the police officer to take a course of action in relation to the new material, or should the officer stop and give the situation wider consideration, which is ordinarily the guidance that is given to police officers?

The Convener: I get that; on one level it can be very simple, but there are all those qualifying conditions. Are you able to share with the sub-committee the internal legal advice that you got from Police Scotland? What format was it in?

Detective Chief Superintendent McLean: It was a memo. I can consider whether it can be shared with the sub-committee; there is obviously a question about doing that with legal advice.

Let me reiterate that, in effect, the advice is that there is a statutory power under criminal justice legislation, supported by case law over the past 10 or 11 years. I have already alluded to two points of case law from about 1997 and 2014, which seem to support the powers that the police used at the time to examine digital devices. That is the advice that was given to us, and the assurances that I have given the sub-committee are, in effect, Police Scotland's internal legal view.

The Convener: I am not sure that I understand why you can share legal advice that was provided by the Crown Office, but not your internal legal advice.

Detective Chief Superintendent McLean: I would probably have to take some direction on that.

The Convener: Do you mean that you will need to take legal advice?

Detective Chief Superintendent McLean: Yes.

The Convener: It would be very helpful if you could do that, Mr McLean, and come back to the sub-committee.

Detective Chief Superintendent McLean: I recognise the issue's importance.

The Convener: During the trial period, which took place without all the supporting framework that is now in place—or it was being discussed, at least—was there any assessment of the potential for retrospective claims? Has anyone come forward and complained?

Detective Chief Superintendent McLean: Not to my knowledge, but I am sure that many people will be watching this meeting with interest. A lot of the discussion is about what police officers are or are not doing and whether they are infringing the various articles of the ECHR. That takes me back to why I might want to take advice about whether we can share some legal advice.

Diego Quiroz: I want to go back to Clare Connelly's point about fishing expeditions. After our previous meeting with the sub-committee, Mr McLean invited me to see how the cyberkiosks work. The police have carefully considered the issue of operational proportionality—the parameters that Mr McLean mentioned—and I am a bit less concerned about legal certainty and the requirement of lawfulness.

Clare Connelly's point relates back to the point about oversight. The reason why we recommend that prior judicial authorisation or an independent body should be the preferred practice for the use of cyberkiosks is that that will provide the independent oversight that is required to ensure that there is none of the practice of fishing expeditions. That also seems to be the preferred approach in cases involving the interception of communications for both the European Court of Human Rights, as seen a month ago in the case of Big Brother Watch v United Kingdom, and the Court of Justice of the European Union, as seen in the Tele2 Sverige AB v Watson case. They clearly seem to favour independent oversight and authorisation processes.

Margaret Mitchell: I want to drill down into the matter of independent oversight. It is clear that that is not a blanket requirement for every mobile phone browsing exercise. How would it work in practice? Would it be required only when something that the mobile phone browsing exercise uncovered was flagged up as being unsuitable?

Diego Quiroz: There are different ways in which it could work. Oversight could be done prior or post, as has been said. It could be done prior, when the authorisation is given, or post, through a review after the authorisation has been given. Such a review would be similar to what happens with protection orders under the Investigatory Powers Act 2016. The orders are given by a police chief superintendent, but the commission reviews the validity and adequacy of the orders post their having been issued.

Margaret Mitchell: There is a big issue there. We are looking at the Police and Fire Reform (Scotland) Act 2012. If there were complaints about whether it was right to carry out the mobile phone browsing exercise, would that not be a strong indication that oversight should take place prior to authorisation being given rather than afterwards? Should the exercise be taken out, so that it is dependent on some issue being raised?

Diego Quiroz: That is the preferable option. It seems that the European Court of Human Rights and the Court of Justice of the European Union are signalling that that is what should happen in the European context.

Rona Mackay: Mr McLean, you have mentioned a couple of times that the device needs to be provided voluntarily. What would happen if you approached an individual and they said, "No, you're not going to get my phone"? Is that as far as it would go, or would that person be marked out as being suspicious because they refused to hand over their phone? I am curious to know what the procedure would be in that case.

Detective Chief Superintendent McLean: The devices are absolutely not intended for us to carry them down to the street and for us to stop people to browse their phones. Principally, they are intended for use when a crime has been reported to the police or when there is some sort of investigation. When I talk about compulsion, I am talking about the victims or the witnesses in those circumstances. We have no powers to require those devices, other than by going through a court to get a warrant if we thought that it was such a grave matter.

Rona Mackay: To clarify, with a suspect, you have that power—it is not voluntary. Is that the difference?

Detective Chief Superintendent McLean: Exactly.

Rona Mackay: That is fine.

Stewart Stevenson: I want to see whether there is a parallel. I am not fully familiar with the Regulation of Investigatory Powers (Scotland) Act 2000 to be certain about the question that I want to ask. Under that act, people can be required to provide their encryption keys. Even an innocent person who refuses to provide the key that would decrypt would become someone who has committed an offence. I am seeing nods. I am trying to explore whether there is a principle in that that we could capture and use in other domains, such as those that we are discussing.

Detective Chief Superintendent McLean: I would love to be able to give a specific answer to that question. The Regulation of Investigatory Powers (Scotland) Act 2000 principally covers a lot of covert activity. You are right: we can require an order for the personal identification number. It is difficult to cover every eventuality. As Mr McArthur mentioned, we are talking about a much wider set of principles with cyberkiosks. It is very difficult to give one set of circumstances that meets every scenario. I go back to the article 2 obligations that policing has in relation to the right to life and high-risk situations. The options that we have discussed have a degree of time wrapped around them, and that is often the complex situation in which police try to operate.

Fulton MacGregor (Coatbridge and Chryston) (SNP): The more evidence that we take on cyberkiosks, the more concerning the issue becomes. Through my work on the Justice Committee and in other areas, I believe that good procedures would probably be put in place, but there is also a public perception, which we have talked about. Through other evidence that the sub-committee has taken, we know that real progress has been made on people coming forward to report certain types of offences, which they might not have done previously, and we do not want to go backwards on those issues. If a committee of MSPs is concerned about the kiosks, I think that the public would be concerned, too. We might have situations in which people say, "I want to report this, but I don't want my whole phone to be checked."

With that point in mind, I want to follow up with a question about training. I believe that the police are continuing to train officers in the use of cyberkiosks. Given the concerns that have been raised and the fact that the use of cyberkiosks may be stalled until further safeguards are in place, is that a good use of police time?

14:00

Detective Chief Superintendent McLean: I take your point. The public concerns go back to the quality of law. We recognise that it is really important to set out the principles and articulate them clearly so that people understand the expectations when they have been arrested for a crime, or when they are a victim or a witness of an incident.

The training decision was about finding a careful balance in the logistical challenge in training more than 400 people. I told the sub-committee that we set out a timeline. Although we are very considered about operational deployment and the go-live, we are also trying to minimise disruption to local policing resources, which is not without challenges. The defining factor in the decision to commence training was that we could properly evaluate whether the training product was fit for purpose, whether we were addressing many of the matters that we have discussed today or have touched on in the margins, and the experience of the officers who were being trained and whether they felt that it was adequate.

The primary driver to commence the training was that it would enable us to carry out a full evaluation. We have started that this week. In the next two to three weeks, we will do a full debrief of the officers to get their feedback and see whether we have got the training right and whether we are catering for the safeguards, checks, balances and considerations that have been talked about here and elsewhere.

The Convener: We have heard from Police Scotland that perhaps it would go about things

slightly differently and about issues such as having a pilot and acquiring the significant capital sum to acquire the equipment. I have a question for all the witnesses that will probably have a simple yes or no answer. Are you content for the cyberkiosks to be rolled out in December, or should we await a definitive yes from the Crown Office and sign-off by the current stakeholder group?

Clare Connelly: They should not be rolled out in December. That is premature. More than a response from the Crown Office is required. The law has to be reassessed and perhaps redrafted to meet the challenges of the use of not only cyberkiosks but technology in the modern world.

David Freeland: We need to be clear about the lawful basis of cyberkiosks. That needs to be expressed to us in clear and straightforward terms. Until that happens, I cannot see that the processing of the personal data would be lawful.

Detective Chief Superintendent McLean: There is a lot of ground to be covered, even if we projected a roll-out in December. However, the discussion hinges not only on cyberkiosks; a much wider discussion is needed, and possibly there is a need for a review and recommendations. We should not frame the discussion solely around cyberkiosks. It looks unlikely that we could roll them out in December. We need to take a very measured approach.

The Convener: Is it correct that Police Scotland would not roll them out without a definitive opinion from the Crown Office? In one of the submissions, Police Scotland said that it might reasonably expect the Crown Office and Procurator Fiscal Service to consider the legal basis for the use of cyberkiosks as

"an operational matter for policing".

However, I am sure that you accept that the interest is broader than just policing.

Detective Chief Superintendent McLean: I am here to represent Police Scotland, and it would be up to the force to make that decision—it would probably start at chief officer level and the SRO for the programme. They would take cognisance of the Crown Office's response as well as all the other contributions that we have received to date.

The Convener: Can you say that it will not begin unless you get the go-ahead from the stakeholder group and the Crown Office?

Detective Chief Superintendent McLean: I cannot make that commitment today.

Diego Quiroz: The answer to the convener's question is no. The current law is not clear; the lawful use of cyberkiosks has no clear basis in domestic law. The law does not have a sufficient quality to be accessible and foreseeable, and that relates to legal certainty. There are no adequate safeguards in place in the law because the legislature did not consider those situations of seizure and search in that context.

The Convener: I thank all the witnesses for their written submissions and for appearing before the sub-committee today—I know that Ms Connelly faced some challenges in doing so. The session has been very helpful. We would appreciate it if Mr McLean could share the material that we discussed.

We will now move into private session.

14:05

Meeting continued in private until 14:23.

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