Office of the Information Commissioner
Queensland

TRANSCRIPT – *Law Enforcement and Public Safety exemption online training*

Part 1 - schedule 3, section 10(1) and (3) of the RTI Act

Slide 01 (0:00)

Welcome to the Office of the Information Commissioner's video on the law enforcement and public safety exemption under the *Right to Information Act.* In this video we are going to be looking at schedule 3, section 10(1) and (3) of the *Right to Information Act.*

Slide 02 (0:17 seconds)

Throughout this video we are going to be referring to the *Right to Information Act* but it's important to remember that exemption provisions under the *Right to Information Act* also apply to access applications made under the *Information Privacy Act.* So these exempt information provisions will apply when you're processing applications under both the *Right to Information Act* and the *Information Privacy Act.*

The *Right to Information Act* does give people the right to apply for access to documents in the possession or control of a Queensland government agency or Minister. We will be referring in this video to agencies throughout but any reference to an agency should be read as including a reference to a Minister.

While it does give people the right to apply for access to those documents it is not a guaranteed right of access and that right must be read subject to the exempt information provisions and the contrary to the public interest factors in the *Right to Information Act.*

Access is to be given unless it is contrary to the public interest to do so and decision makers are required to have a pro-disclosure bias when they're making those decisions.

When deciding whether it's contrary to the public interest to release information, Parliament has already decided that where the exempt information provisions are concerned it is contrary to the public interest to release any information that falls within those provisions.

Slide 03 (1:42 mins)

What we're going to be looking in this video is one of those specific exempt information provisions and it's one of the bigger ones. The exempt information provisions are all contained in schedule 3 of the *Right to Information Act.* We're going to be looking at schedule 3, section 10. As I said, it is one of the larger of the exempt information provisions and it creates what I'm going to refer to as a class of exempt information. All of them relate to law enforcement and public safety matters. They go from 10(1)(a)-(k) so that gives you an idea of exactly how large this exempt information provision is. What we're going to cover is 10(1) and that goes from 10(1)(a)-(k) and we're going to look at briefly 10(2) and 10(3). We are not going to cover the Crime and Corruption Commission exemption and we're not going to look at the rest of schedule 3, section 10. If you need any information on any of those you can look at the Guidelines or the annotated legislation or you can contact the Enquiries Service and we will do our best to assist you.

Slide 04 (3:03 mins)

Schedule 3, section 10(1) lists a significant number of classes of information that will be exempt from release. What schedule 3, section 10(2) does is lists information that will *not* be exempt under section 10(1). If you've got something that fits under the provisions in schedule 3, section 10(1) but it also fits under schedule 3, section 10(2), it will not actually be exempt. I'm not going to go through these in any detail; I'm just going to flag them so you're aware of them. I don't believe they come up very often, but if you are running any of the schedule 3, section 10(1) exempt information provisions it's going to be important that you have a quick look at schedule 3, section 10(2) an confirm that none of them apply in your circumstances.

Even if something falls under schedule 3, section 10(1) it's not going to be exempt:

- if the information reveals that the scope of the law enforcement investigations has exceeded the limits imposed by law
- if it consists of a general outline of the structure of a program adopted by an agency for dealing with a contravention or possible contravention of the law
- if it simply consists of a report on the degree of success achieved in a program adopted by an agency for dealing with a contravention or possible contravention of the law.

Slide 05 (4:37 mins)

- if it's a report prepared in the course of a routine law enforcement inspection or investigation by an agency whose functions include that of enforcing the law (this does not include criminal law or law relating to corruption under the *Crime and Corruption Act 2001*); or
- if it's a report on a law enforcement investigation that has already been disclosed to the entity the subject of the investigation.

That's all I'm going to say about them as I just wanted to flag that those exceptions to the exemption exist. If you're running any of the exempt information provisions in 10(1) have a quick look at 10(2) – think of it as a checklist. Yes, none of these apply that I'm exempting or if one of them does apply you're obviously going to have to think long and hard about whether or not you can still exempt it. Just because something is not exempt under 10(1) it may still be contrary to the public interest to release or possibly exempt under another information provision in schedule 3. You do need to be aware of them and you do need to run that checklist to make sure the information is exempt.

Slide 06 (5:52 mins)

In case you hadn't gathered from all of the words on the slide – this is about "reasonably be expected to". One of the things that all of the provisions in schedule 3, section 10(1) have in common, apart from being related to law enforcement and public safety, is they all have the tagline "could reasonably be expected to". The actual wording of schedule 3, section 10(1) is that …'*information is exempt information if its disclosure could reasonably be expected to'…* and then it goes on to list (a)-(k). The test is not an absolute test. It's not "it would definitely happen". It is only that the disclosure could reasonably be expected to have one of the effects listed in (a)-(k).

I just want to take you through what that means: *could reasonably be expected to*. It does in fact apply to every single one of the provisions in section 10(1)(a)-(k). Going through every single one of those would seem to be a waste of both my time and yours. I appreciate you taking the time to listen to me and I would prefer not to waste any your time so we are going to go through it now at the beginning.

Slide 07 (7:29)

So what does 'reasonably be expected to' actually mean? The outcomes will be reasonably be expected to occur from the information's disclosure if they are reasonable as distinct from something that is irrational, absurd or ridiculous. That's from an Information Commissioner decision: *VHL and Department of Health*.

There must be real and substantial grounds for the expectation; a mere possibility, speculation or conjecture is not enough. It has to be more than a mere possibility. There has to be something more than that it could occur, it's not necessary that you must be satisfied on some balance of possibilities that the effect is going to definitely crystallise into actually happening. There's a bit from a case called *Neary and State Rail Authority*[1] which is in the annotated legislation which sums it up quite well. In it they say…

> *… There must be more than a mere risk. While the key word used in the relevant provision - `expect' - carries a firmer connotation than words such as `anticipates', it is not necessary that the level of risk be such that it be assessed as more probable than not. Nor is it necessary for the administrator to apply a balance of probabilities calculus similar to that used to set the burden of proof in litigation. All relevant factors, including public interest considerations, should be taken into account. The extent and nature of the effect will be relevant, and often decisive. It is necessary to assess what is reasonable in the circumstances.*

I think that last bit is probably, in the RTI context, one of the most important things when applying this exempt information provision – it's what's reasonable in the circumstances. There's nothing in applying this 'reasonably be expected to' test in 10(1) that's substantially different from making a decision under any other exempt information provision or applying any combination of public interest factors. For everything you have to be able to point to something and say "yes, on that basis I think that this is likely to happen". You do have to have some sort of a basis for making your decision when you're deciding that you have a reasonable expectation, it could reasonably be expected, that one of the effects in 10(1)(a)-(k) could be the outcome of disclosure of the information.

When you're considering any of the provisions in (a)-(k) you will have to keep that in the back of your mind that the outcome is reasonable as distinct from something that is irrational, absurd or ridiculous. I'm going to say this far more times than you're actually going to want to hear it but I think it's very important to remember, particularly in light of the fact that we are dealing with a provision that relates to law enforcement and public safety, some of the issues that are touched on by these provisions can involve a lot of serious matters. The effect that we are looking at, the expectation, has to arise from the disclosure of the information and not from any other circumstance. If the threat to physical safety, the threat of serious harassment, the threat to the security of the building is coming from any other source or circumstance other than the disclosure of the information then the provision simply can't

[1] Which is in the annotated legislation here: *Could reasonably be expected to*

apply. The expectation must be arising as a result of the disclosure and that is key to all of the exempt information provisions in 10(1)(a)-(k).

Slide 08 (**12:11)**

Content of slide:

- *it is an objective test, taking into account the content of the information*
- *a decision maker must consider whether the particular outcome in section 10(1) could reasonably be expected to occur as a result of the disclosure*
- *Consider:*
    - *Is the expectation reasonably based?*
    - *Is the outcome reasonably open, having regard to the disclosure of the information?*

Slide 09 (12:12)

So kicking off with 10(1)(a): information is exempt if its disclosure could reasonably be expected to prejudice an investigation into a contravention or possible contravention of the law. Throughout 10(1) where there's references to contravention of the law, they always include a possible contravention of the law and it's also explicitly said to include revenue law. Any reference in this presentation to contravention of the law includes a possible contravention of the law including revenue law.

That makes sense if you think about it because depending on where the investigation is up to and the nature of the law in question it may be impossible to say that the law had in fact been contravened. Generally that is the whole purpose of an investigation is to determine whether or not a law has been in fact been broken.

Slide 10 (13:18)

One of the other things to remember when we are talking about law here (and one of the reasons I will probably never again ever mention revenue law) is that the law being investigated does not have to be the criminal law. It extends to any law that imposes and enforceable legal duty to do or refrain from doing something. This can include civil law or misconduct investigations. It can include investigations by environmental compliance officers into breaches of environmental regulations or licence contraventions. It can include investigations by local government officers into breaches of the law, particularly an example that springs to mind like investigating complaints about dog barking or people being attacked by dogs. Investigations into breaches of liquor licencing laws. Essentially any time there is a law in place that can be broken or any sort of enforceable legal duty that someone can fail to do – these provisions can apply. It does not have to be the criminal law. Because this is the approach that has been taken under the *Right to Information Act* obviously that will include revenue law as well. This applies for every provision in 10(1) that refers to contraventions or possible contraventions of the law.

Slide 11 (15:15)

Investigation isn't defined in the RTI Act so it gets its ordinary meaning which is:

- The act or process of investigation.
- A searching inquiry in order to ascertain facts; a detailed or careful investigation.

Keep in mind, if an investigation is finalised this exemption will generally not apply. I know that it can often be difficult to determine when an investigation is finalised particularly in some situations where perhaps something might have been filed in court yet the investigation may still ongoing. There can be a grey area around the end of that investigation. I am not going to pretend to be able to give you a final, absolute, definitive answer as to when an investigation has come to an end in this format here. I think pretending I can do that in this sort of environment, no, I can't do that, because there's always going to be a circumstance that will be an exception. If you do have questions or you've got a situation where you're not sure if the investigation is finalised, you can contact us on the Enquiries Service and we will do our best to assist. Having a look at the annotated legislation and the Guidelines and previous decisions can also help with that. I will absolutely acknowledge to you that there are grey areas when an investigation is finalised. In most cases it's very clear but there can be those occasional grey areas.

Slide 12 (17:08)

I've pulled a couple of cases just to highlight some differences in the severity of the prejudice that can attach to the investigation and have this exempt information provision apply. The situation in *Latemore and Department of Police* was that information would have *"severely jeopardise(d) the integrity of the entire investigation"* and so the information was exempt from release. In *Cudmore and Queensland Police Service* disclosure would have placed the investigators in a more difficult position than they otherwise would have been when questioning the applicant or his alleged accomplice about the alleged offences and it was exempt from release.

So you can see that it's a, let's call it a sliding scale of prejudice, it doesn't have to be a death knell for the investigation to exempt. It merely has to prejudice the investigation. The thing to ask is "will disclosure undermine or disadvantage the investigation?" Prejudicing the investigation doesn't mean it's going to be a death knell.

Slide 13 (18:16)

10(1)(b) is about confidential sources of information. Information is exempt if its disclosure could reasonably be expected to:

- enable the existence or enable the identity of a confidential source of information
- in relation to investigating or dealing with a contravention or possible contravention of the law.

The purpose of this section of the RTI Act is to ensure that citizens are not discouraged from cooperating with agencies engaged in the enforcement or the administration of the law and that they continue to provide information which might assist such agencies to more effectively perform their functions. It make sense if you think about it: if you come forward as a confidential source to Queensland Police Service, Corrective Services, Department of Natural Resources, Environment and Heritage Protection etc. and you aren't able to trust that they will keep your existence/identity as a confidential source confidential the chances of anyone coming forward and agreeing to be a confidential source in the future is pretty slim. There's a certain amount of trust that needs to exist before people are going to be willing to come forward. People supplying information is a fairly important part of enforcement and that's essentially why this provision exists.

Slide 14 (19:43)

For information to be exempt under this provision it must:

- be supplied by a confidential source of information
- relate to the enforcement or administration of the law; and
- be reasonable to expect disclosure could enable the existence or the identity of the confidential source to ascertained.

For the source to be confidential there can have been an **explicit** understanding that their identity would be kept confidential or an **implicit** understanding that their identity would be kept confidential. It's much, much simpler if there was an explicit understanding but it is not necessary 100% that exist for them to be a confidential source. There can be, based on the circumstances, an implicit understanding they are a confidential source.

Slide 15 (20:38)

For an explicit understand of confidentiality the source was told their identity would be confidential. That's nice and simple. For an implicit understanding you need to look at:

- The nature and circumstances of the information provision.
- Any relationship between the parties. Now that could be: the source and the agency, the source and the alleged offender, the source and any people involved in the alleged offence. You can be looking at a number of parties and any expressed wishes of the source that it be kept confidential.
- Any detriment that could accrue to the source of the information. When you're considering whether or not there was an implicit understanding that they could be kept confidential.
- You could also have a look at whether the information provider is comparable to an informant, for example a whistle-blower or a witness. Not if they were *actually* a whistle-blower under the current equivalent legislation as that would raise a whole different kettle of fish but whether they are an equivalent to that.
- Whether it could have been reasonably understood by both the information provider and the agency that the agency could have taken action on the information that source provided without identifying them.
- You can have a look at the manner in which the information was imparted.

Essentially if you're trying to identify whether there was an implicit understanding of confidentiality look at all the circumstances surrounding the information provision. As always, the people in the business units who are dealing with the files and with the sources can be a very valuable source of information. It's always important to speak to them about what they understood if you're having any doubts.

Slide 16 (22:33)

Once you've done that and you have determine that the source was confidential (whether explicitly or implicitly) the information still has to have been given in the course of the investigation or the administration of the law. You still have to determine that keeping in mind that it doesn't have to be criminal law and it can be contravention of possible contravention.

Once you've determined that you have to ask: would disclosure reveal that confidential source exists or identify that confidential source. If yes, the information will be exempt from release.

One of the things that every single decision maker has encountered is the applicant who says "but I know who it was. I know! I know it was X/Y/Z". Sometimes they might be right it may have in fact have been X or Y or Z. A lucky guess is a lucky guess or reasoning from first principles – the balance of probabilities it had to be X or Y or Z. That is not really enough to remove the person as confidential source. People can make educated guesses or run a process of elimination and seek official confirmation of their guess or elimination process through an RTI application. It's true that this provision couldn't apply where the applicant *knew* who the confidential source of information was. But there's a big difference between educated guess and "I know because I have some sort of official document from the agency that says who they were" or "I was told by the investigator" and they have some sort of evidence to prove that "I know who the confidential source was." An educated guess is an educated guess and most decision makers have encountered the applicant making an educated guess and seeking confirmation through the RTI process. If an access applicant is making an application and saying they know who the confidential source was – without some sort of evidence (preferably evidence from your own agency) that they do in fact know, this provision will still apply. At the end of the day, absent that evidence, it's simply an educated guess or an extraordinarily lucky one.

Keeping in mind if the person applies for information about a confidential source of information by name ("I want all documents about Sharron Harrington's information provided to the department about my illegal activities") of course the appropriate response there would likely be "neither confirm nor deny" – but that's a completely different video for a completely different day. The important thing to keep in mind is that an applicant who claims to know without evidence should be treated as any other applicant and this provision should be run in the standard way.

The other thing that sometimes comes up in relation to this provision is: what if the information from the confidential source was supplied maliciously or it's false? It's important to remember that's not a relevant consideration under this provision. If you meet all the tests for 10(1)(b) the source is confidential; the information was provided in the course of an investigation or administration of the law; disclosure would reveal the confidential source exists or would reveal that source then this exempt information provision applies. It is in fact irrelevant whether the information provided by the confidential source was false or was provided maliciously. It is completely irrelevant to this section and is not something that should be taken into consideration. If it's raised by an access applicant then it's really up to you how you choose to deal with it. But you can run this section if it applies and it's just simply not a relevant consideration.

Slide 17 (27:32)

10(1)(c) is about the endangering of life or physical safety. Information is exempt if its disclosure could reasonably be expected to:

- endanger a person's life; or
- endanger a person's physical safety.

It is important to remember that the source of danger does not have to be the access applicant for this exemption to apply. The access applicant does not have to be the person that will represent the

threat to someone's life or someone's physical safety. The threat can come from anywhere and it can be a specific threat or it can be a more general threat.

Slide 18 (28:10)

The key here is that there must be:

- a source of danger to a person or a person's life or physical safety; and
- there's some evidence of a risk that disclosure would endanger person's life or physical safety.

When you're looking at this provision you will need to consider all of the relevant evidence, including any evidence that might be supplied by the person claiming to be at risk and any evidence obtained about the alleged source of danger. One of the things to keep in mind is that this could be a specific life or a more general danger.

One of the decisions that has been made by the Queensland Information Commissioner was *Courier Mail and Queensland Police Service* and this provision was run and upheld. The information in issue related to suicide attempts and successful suicides and specific locations where these had been attempted and successfully attempted. The argument was run that if this information was released it could lead to an increase in suicide attempts at those locations. This was upheld on the grounds that disclosing the information could reasonably be expected to lead to an increase in the number of people who either attempted or completed acts of suicide at the specific location and therefore it was exempt under this provision.

The way the provision is worded does tend to focus the mind in on a threat to a specific person's life or a specific person's physical safety but it's important to remember that this can be a more broad or general provision when you are considering that sort of information. So you can look at life or physical safety on a much more holistic approach. You still have to satisfy all of the elements but you don't have to be able to point to a specific person and say "yes, that person's life is in danger/that person's physical safety is in danger". You can say, people's lives generally or people's physical safety generally would be endangered or could reasonably be expected to be endangered if this information was disclosed. Do keep that in mind when you're looking at documents that may involve a more general threat to people's lives or physical safety.

Slide 19 (31:22)

The other thing to remember is that in some cases the access applicant them self may be the one whose life or physical safety could reasonably be expected to be endangered by the release of the documents. In those circumstances it may be appropriate to run this but it also may be appropriate to look at alternative RTI mechanisms. Where the documents in question are health records it may be more appropriate to run a healthcare decision to protect an applicant. Just some things to keep in mind. From the way the provision is written I think it is natural for one's mind tends to look towards a third party endangered by the applicant but it can be life generally. It can be the access applicant's life, it can be essentially anyone's life or physical safety if it can reasonably be expected to be endangered by the release of the documents. I think it is a much broader provision than it appears on first reading. Hopefully it's not something you'll ever have to run but if you do encounter circumstances where you do feel that life or physical safety could be endangered from the release of

the documents you could have a look at this provision and see if it does stretch to cover your circumstances. As always, the Enquiries Service is there to help if you want to toss ideas around.

Slide 20 (33:00)

10(1)(d) – serious act of harassment or intimidation. The thing about 10(1)(c) (endanger life or physical safety) is there's been a couple of decisions that have said a serious act of harassment or intimidation is *not* enough to trigger 10(1)(c). But that's ok because we have 10(1)(d) – serious act of harassment or intimidation, which says that information is exempt if its disclosure could reasonably be expected to result in a person being subjected to:

- a serious act of harassment; or
- a serious act of intimidation.

The terms of the sections aren't defined by the RTI Act so, as always, when a term in an Act is not defined by the by either the RTI Act or in the Acts Interpretation Act, we look at the ordinary meaning.

Slide 21 (33:51)

The dictionary has helpfully defined these.

Harass: *to trouble by repeated attacks, to disturb persistently; torment*

Intimidate: *to make timid or inspire with fear; overawe; cow, to force into or deter from some action by inducing fear*

Serious: *giving cause for apprehension; critical, having (potentially) important, especially undesired consequences; giving cause for concern*

Slide 22 (34:21)

These definitions have been consistently used by the Information Commissioner. Under the FOI Act (now repealed but 10(1)(d) essentially replicates the FOI provision) the Information Commissioner specifically observed that acts which induce fear or force a person into some action by inducing fear or apprehension are acts of intimidation. Acts of intimidation which have undesired consequences or cause concern and/or apprehension are serious acts of intimidation. Acts which persistently trouble or disturb or torment a person are acts of harassment. Acts of harassment which have undesired consequences or cause concern and/or apprehension are serious acts of harassment. That's from *Sheridan* and the other important thing that the Information Commissioner said in *Sheridan* is the exemption can apply even where a single act of serious harassment is expected to occur. In many of the cases and situations where 10(1)(d) applies, often you're looking at a series of actions or a series of acts (escalating or otherwise). That is in most cases where people are going to run 10(1)(d). It's not 100% necessary because as the Commissioner said in *Sheridan* it can apply even where a single act of serious harassment is expected to occur.

Slide 23 (35:50)

When you're looking at relevant factors to apply in 10(1)(d) you look at:

- past conduct or a pattern of past conduct
- the nature of the information in issue

- the nature of the relationship between the parties/third parties
- any relevant contextual and/or cultural factors

Remember, in this provision and any other provisions in section 10(1), the applicant's subjective purpose for applying for the information is irrelevant. The only thing that matters if the effect that disclosing the information may have. That is the case for all of section 10(1). It is the effect of the disclosure that matters not the applicant's purpose in applying, not the effect of any other intervening action or other circumstances.

Slide 24 (36:44)

The fact that it has to be a *serious* act of harassment or intimidation does actually imply that some degree of harassment or intimidation is permissible before access rights are removed. It has to be a *serious* act of harassment or intimidation and we talked before about what serious requires.

The other thing to keep in mind is that you don't have to be able, in order to run this provision, to draw a causal link between the applicant or between a specific person for the conduct for the exemption to apply. In most cases you will. You will be able to point to someone or to their name on the page and say, "yes, that is the person who is the harasser or the intimidator", but it is not 100% necessary to be able to do that. It is enough that disclosure *could* result in person being subjected to a serious act of harassment or intimidation.

As I mentioned before, it is the disclosure itself that must be the trigger for the conduct in order for the exemption to apply not some intervening third action.

I just want to mention a couple of cases just to highlight how the serious act of harassment or intimidation can be different than what we might expect it to be. *Richards and Gold Coast City Council* is a good one for what I'm going to call a standard act of harassment or intimidation. I don't mean in any way to belittle or underplay how serious a serious act of harassment or intimidation is when I describe it as a standard. What I mean in that way, is the method by which the harassment and intimidation was undertaken. In *Richards and Gold Coast City Council* the harassment and intimidation was undertaken by telephone. Multiple phone calls to council staff and elected representatives both inside and outside of work to mobile and private phone numbers, making implicit and explicit threats of violence against staff members, elected representatives, and their family members. This was someone who undertook serious acts of harassment or intimidation directly against individuals using the telephone. They made an application and the information they applied for was found to be exempt essentially on the grounds that their pattern of past conduct was enough to infer that there would be future patterns of conduct along those same lines. The information they'd applied for had elicited extremely strong reactions in the applicant before and if it was released it was likely to elicit those same strong reactions in the applicant and likely to lead to a pattern of future conduct of serious harassment and intimidation similar to the past conduct of serious harassment and intimidation. The applicant had been in dispute with Council for many years and the applicant's conduct had detrimentally impacted council staff and elected representatives – information was found to be exempt under this provision. The thing I want you to take from there is that the serious acts of harassment and intimidation were taken *directly* against individuals using the telephone.

I want to contrast that against *Mathews and the University of Queensland* which is quite different. In this case, the applicant never directly seriously harassed or intimidated the staff of the agency. What

the applicant did was build a website, named agency staff, made extremely offensive comments about them, offensive statements, attacks and accusations to be specific and then stated the website was specifically designed to achieve a high Google ranking so that if anyone searched for those agency staff the website in question would be one of the first hits. The applicant specifically stated that this was intended to negatively impact on them: their life, their job prospects and that sort of thing.

In making her decision, the Acting Information Commissioner specifically stated that she did not take the motivations of the applicant in making the access application into account but she did take into account the motives of the potential harasser or intimidator. In this case they happened to be the same person but as I mentioned before it's not necessarily going to be the case. The Information Commissioner was satisfied that disclosing the information would reveal the identity of individuals (staff members) and it could reasonably be expected to result in those individuals being subjected to serious acts of harassment or intimidation. Namely, being placed on the applicant's website and having the same unfounded allegations and offensive commentary attached to their names. Based on the malicious nature of the applicant's website, including its stated purpose, together with the impact that it had on the individuals targeted it was sufficient to conclude that postings on the website constituted serious acts of harassment and intimidation. So that is a very different type of action than the one taken in *Richards and Gold Coast* which is a sort of standard act of serious harassment or intimidation – direct threats and harassing of people using the telephone. In the case of *Mathews and the University of Queensland* he didn't directly contact, as far as I know, if it happened it was in no way relevant to the decision. He wrote about them on his website and used what must be a reasonably sophisticated method of building a website to have it listed high on Google rankings to harass and intimidate people. Like a serious threat to life and safety when you read "serious act of harassment and intimidation" I think it's natural to read it as a person seriously harassing or intimidating another person in a standard way. In most cases that is likely to be the situation in which you are going to be running the exempt information provision but again, like 10(1)(c) – serious threat to life or safety, there can be other circumstances in which it could apply.

Slide 25 (44:59)

10(1)(e) – prejudice a fair trial or adjudication. Information is exempt if its disclosure could reasonably be expected to:

- prejudice a person's fair trial; or
- prejudice the impartial adjudication of a case.

In this case, fair trial refers *only* to a criminal trial. That part of 10(1)(e) can only apply where criminal trial is in contemplation. Impartial adjudication, however, refers to any dispute adjudicated by an impartial decision maker. I'm not going to spend a lot of time on this one. To the best of my knowledge, it doesn't arise particularly often. It can only apply if a specific criminal proceeding or a specific case to be adjudicated is identified. You can't run this as a general principle or a holistic idea that you can't release this information because the *idea* of a fair trial would be endangered. You have to be able to specifically pinpoint a specific fair trial or a specific case the impartial adjudication of which would be prejudiced. One of the things that the Acting Information Commissioner said in *North Goonyella Coal Mines Pty Ltd and Millard and Department of Natural Resources and Mines* was that she could not be satisfied on the evidence that disclosure could reasonably be expected to prejudice a person's fair trial given that the applicant's representatives were legal professionals obliged to

behave properly and ethically when presenting issues to court. The court is capable of determining the relevance of issues in arguments presented to it by either party and the court is equipped with appropriate mechanisms to deal with any conduct it identifies as attempts of investigation or designed to side-track the prosecution. The things to take away from that is that running this is a fairly high bar to meet because by its very nature going to a trial or an impartial adjudication of a case means that proceedings are going to be overseen by someone whose job it is to ensure that matters proceed fairly. Where lawyers are present they have a duty to the court above all else and are held to high ethical standards. So running this it is going to be a fairly high bar to meet so I would tread carefully. Have a look at the annotated legislation if you do think it's going to come up or you need to make arguments why it doesn't apply and also have a look at the Guidelines. As always, you can contact the Enquiries Service but that's pretty much all I'm going to say about that one.

I think this might be an excellent time to break so I'm going to stop here. If you've decided to watch all the way through onto the second one go and have a cup of coffee or take a little break and we will be back shortly.

[END]

Office of the Information Commissioner
Queensland

TRANSCRIPT – *Law Enforcement and Public Safety exemption online training*

Part 2 - schedule 3, section 10(1) and (3) of the RTI Act

Slide 01 (0:00)

Welcome back to the Office of the Information Commissioner's training video on the *Right to Information Act* schedule 3, section 10(1) - law enforcement and public safety exemption. This is Part 2 of a two part video series. If you haven't seen part 1 why are you watching part 2? Go back and watch part 1, I'll wait…excellent, you've watched part 1, now welcome back to part 2. Part 2 isn't going to make a lot of sense without having seen part 1.

Slide 02 (0:34)

The last thing we covered in the video in part 1 was 10(1)(e) and we covered it very briefly. So going to 10(1)(f) and (g), which I'm covering together, is about contravention of the law and protecting public safety.

Under 10(1)(f) and (g) information is exempt if its disclosure could reasonably be expected to prejudice:

- the effectiveness of a lawful method or procedure for preventing, detecting, investigating or dealing with a contravention or possible contravention of the law; or
- the maintenance or enforcement of a lawful method or procedure for protecting public safety.

Prejudice means to *detrimentally impact.* Remembering that contravention or possible contravention of the law doesn't just mean criminal law it means all of the laws.

Slide 03 (1:30)

The reason I'm covering these together is because for both of them to apply, there must be an identifiable lawful method or procedure in place. I'm not going to spend a lot of time covering it but the method or procedure must be lawful. This won't apply where the investigators have gone off the rails and are following an unlawful method or procedure, for example, they've got a secret illegal wire-tapping thing going on – this exception is not going to protect their illegal wire-tapping procedure. It must be a lawful method or procedure. It must be a specifically identifiable method or procedure.

- This can be a written policy or procedure
- It can be a voluntary process in place
- Less obvious arrangements can also qualify. Something that you wouldn't normally look at and say "ah yes, that is a method or procedure". For example, police rosters. In *Gold Coast Bulletin and Queensland Police Service* they were exempt because they were a lawful method or procedure. Some of the reasons for that were because:
    - they were created by senior staff
    - they reflected the operational requirements of the station and methodologies employed to meet those requirements; and
    - they accounted for specific challenges relevant to the particular policing division in which they were in place.

So in that case police rosters were recognised as being an identifiable lawful method or procedure.

On a first reading of the requirements of lawful method or procedure you'd be thinking of things like written polices or processes or procedures but they can be much broader than that.

Slide 04 (3:25)

Looking specifically at 10(1)(f) we are looking at identifiable and lawful methods and procedures relating to the prevention, detection, investigations or dealing with a contravention of the law. The prejudice that would be reasonably expected to occur must be to the *effectiveness* of the procedure. The procedure must be used by the agency for preventing, detecting, investigating and/or dealing with contraventions or possible contraventions of the law. There must be a reasonable basis to believe that disclosure of the information would reduce the effectiveness of the procedure. So we are specifically looking at reducing the effectiveness of the procedure.

Slide 05 (4:17)

This exemption will often arise when the agency has adopted covert, secret, or only internally known procedures or methods and public awareness or even greater awareness of these procedures could reasonably expect to make them less effective in the future. It's not going to generally apply to routine methods or procedures. For example, it's common practice for agencies to interview witnesses to obtain information that's needed for an investigation. If you're conducting an investigation and there's witnesses to the alleged offence then you're going to interview witnesses to find out what they know. Accordingly, the fact that you have a procedure that says 'investigate witnesses' is not going to be something that would be exempt under this provision. I think it's reasonable to say everybody knows that as part of an investigation you interview witnesses; disclosing it would not reasonably make that less effective. If there was something in that witness interviewing procedure that, if that were publicly known, would make your ability to interview witnesses less effective in the future. It would be reasonably be likely to prejudice the effectiveness of your witness interviewing procedure then it is possible that could be exempt from release under this provision. But the mere fact that you have a procedure and it says 'interview witnesses as part of the investigation' would not be sufficient to quality: that would be a routine method or procedure.

The simple fact that a method or procedure has previously been disclosed doesn't necessarily mean that information relating to that method can't be exempt under this provision. It could be that the method had previously only been used in limited circumstances, maybe to trace a drug suspect, and people wouldn't expect it to be used in other circumstances. It's all about looking at all of the circumstances of any previous disclosures of the information to determine if it had reached a point where it was publically known or so well known that any secrecy around the procedure itself had been removed. Previously limited disclosure of information about method or procedures may not mean that it's widely known by the public. This could particularly be the case if the information had taken place amongst colleagues or peers, for example if people in one agency involved in particular sort of investigation shared their methods or procedures with peers in another agency involved in a similar sort of investigation. I think it's unlikely that that level of sharing would remove the ability to exempt information under this provision. It's highly unlikely that a fellow investigator is going to do anything to reduce the efficacy of the investigative procedure. One example you can look at is *VO and Department of Health*. It was an FOI decision but again the FOI provision is basically replicated in 10(1)(f). In that case the information that was refused access under this provision that was upheld by the Information Commissioner was the disclosure of the applicant's file from the drug dependency

unit. It was upheld that disclosure could reasonably be expected to prejudice the effectiveness of the methods used by the Department of Health to monitor persons using dangerous drugs. In that case we are looking at the entirety of an applicant's file as the method which was being protected, not a procedure. The Information Commissioner found that the effectiveness of the monitoring methods could reasonably be expected to be prejudiced because the information, if disclosed, could be used to obtain dangerous drugs and to do so without detection. Public awareness of that method could have reasonably been expected to make it less effective in the future.

Slide 06 (8:57)

When we are looking at protection of public safety which is in 10(1)(g) the prejudice that we are looking at is to the *maintenance* or *enforcement* of the method or procedure. This is different from the *effectiveness.* Not all methods or procedures are going to be enforceable. If a method or procedure is not enforceable, look at whether it is maintainable. In *VO and Department of Health* the method of monitoring persons using dangerous drugs is arguably not enforceable – it is a method for monitoring someone. You can look at whether it is maintainable, that is whether it can be enable to be continued. The purpose of the method or procedure must be for the protection of the public. This could be the public generally or it could be a specific subset of the public. One of the main cases where this has been applied under the RTI Act was *Nine Network Australia and the Department of Justice and Attorney General*. This case basically turned around information provided voluntarily by people who operate amusement park rides. Essentially the Information Commissioner did find that it was a lawful method or procedure for protecting the public safety, in so far as that amusement ride operators were providing information to Workplace Health and Safety voluntarily to aim at improving the safety of persons who use amusement devices and achieve best industry practice. There was no doubt that it was an identifiable lawful method or procedure for protecting public safety. It fell down on the second part of the test that releasing it would prejudice the maintenance or enforcement of the method of procedure but that doesn't really matter for the purposes of this discussion. In that case it was the subset of the public i.e, people who use amusement park rides. Despite the fact that it was voluntary it was in fact a lawful method or procedure for the protection of public safety.

Slide 07 (11:22)

Prejudice not being defined in the RTI Act is given its ordinary, natural meaning which is to detrimentally impact. A method or procedure will be prejudiced (or detrimentally impacted) if its efficacy will be reduced by the disclosure. So essentially it will be less effective. Examples of expectation of prejudice to the relevant system/procedure:

- Disclosure would result in potential informants being less likely to provide relevant/quality future information.
- Disclosure would result in people being discouraged from making calls to emergency services.

Those are examples where if the method or procedure had been disclosed that would have been the result which would have meant that the method or procedure would have been less effective because obviously the method or procedure had been designed to have those particular outcomes. The method or procedure was designed for people to provide relevant or quality future information and if it was disclosed that wouldn't have happened. Or the method or procedure was designed to make sure people felt confident making calls to emergency services and if it was disclosed they would have

been discouraged from doing so which would have made it less effective. As always, the expectation of prejudice must exist as a result of the disclosure not from any other circumstance. I know I've said that multiple times but it's very important to remember that for all of these exempt information provisions in 10(1) the effect listed in 10(1) must come from the disclosure and not from any other intervening circumstances or the effect could reasonably be expected to come from the disclosure and not from any other intervening circumstances.

Slide 08 (13:13)

10(1)(h) – I'm not going to spend too much time on this one. Information is exempt if its disclosure could reasonably be expected to endanger:

- the security of a building
- the security of a structure; or
- the security of vehicle.

The potential danger must exist as a result of the disclosure and not from any other circumstances.

Slide 09 (13:45)

The Information Commissioner has previously considered a number of situations in which this exemption may or may not apply. Here are some of them:

- residential house – yes it can apply. In that case it was regarding building plans and whether or not having possession of them would make it simpler to break in
- a prison – yes, that seems fairly obvious
- the Maximum Security Unit of a prison – yes, again that seems fairly obvious
- an itinerant food van – no
- parking meter machines – no; and
- hotels, clubs and casinos – no. I'll be very disappointed if somewhere out there someone listening to this didn't immediately think "but what about Ocean's Eleven?" I have no way of knowing…if you did think immediately about Ocean's Eleven please email the Enquiries Service and let me know.

  In the case of someone making an application for documents about a hotel, club and casino that triggered someone thinking about this particular provision the Information Commissioner found the information was not exempt – it was in very specific circumstances. There would absolutely be circumstances in which someone might apply for the building plans of a hotel, club or casino and the information could very well be refused on these provisions. In this case it wasn't.

Slide 10 (15:20)

In order for this provision to apply there must be an identifiable building, structure or vehicle and disclosure of the information could reasonably be expected to endanger its security. Generally you're going to have to be able to identify the precise nature of the threat to security. Just general hand waving "ooo it's a threat to security" probably isn't going to be enough. It may be evident from the information and it will often be affected by the specific circumstances. In the case of the previous casino example (you know, where I couldn't stop talking about Ocean's Eleven), the Commissioner

considered the information's age, the fact it was a single page of information, what other information was publically available having regard to the information applied for and the likelihood of existing criminal activity of similar venues and said that this provision didn't apply. So, no, the Information Commissioner was not enabling an Ocean's Eleven style heist at a particular casino. I promise I'll stop talking about Ocean's Eleven now.

You'll have to look at all of the circumstances of the particularly information. If you are going to run it then something more than just "it could be a threat to security" is going to be necessary. You're going to have to say *this* sort of security or something more than just vague *security* security is going to be necessary to run it. Obviously if someone is applying for the plans of an explosives storage base or maximum security prison or anything along those lines it's going to be fairly obvious that this provision is likely to apply. If someone's applying for structural plans, or perhaps rosters, or the routes security guards take, or anything along those lines, that's likely to trigger the contemplation of this sort of provision and likely also to identify the nature of the threat to security. I vaguely remember someone applying for the building plans of the Helidon Explosives Reserve when I was a decision maker and I'm fairly certain we ran the FOI equivalent of this provision and that was pretty much the end of it – it was fairly obvious. That's probably all I want to say about that provision.

Slide 11 (18:09)

Information is exempt if its disclosure could reasonably be expected to prejudice a system or procedure:

- for the protection of persons
- for the protection of property; or
- for the protection of the environment.

Prejudice and *lawful method or procedure* are going to be exactly the same as at 10(1)(f) and (g).

Slide 12 (18:32)

The system or procedure must be identified and assessed to determine whether it is *'for the protection of persons, property or environment.'* Again the procedure or method must be a lawful procedure or method. This is a question of fact. Examples of some things that could be procedures or methods for the protection of persons, property or the environment:

- The Triple-Zero system.
- Measures taken by the Queensland Art Gallery to preserve the confidentiality of its art values.
- Corrective Services' Intelligence Group's intelligence database.

If you're applying the section you're going to go through the same steps you went through with (f) and (g): identifying a specific procedure or method; making sure it's lawful; assessing whether it's for the protection of persons, property or the environment; assessing whether disclosure can reasonably be expected to prejudice the effectiveness of that method.

Slide 13 (19:32)

Information is exempt if its disclosure could reasonably be expected to facilitate a person's escape from lawful custody. This exemption is generally going to involve information either created by, or acquired from, agencies that put security arrangements in place to keep people in custody – eg Corrective Services, Queensland Police, maybe some youth justice organisations, anything like that. Generally that is going to be where the information is held by or where it's come from because there's a very limited number of agencies that are going to be involved keeping people in lawful custody.

Slide 14 (20:15)

Information that has been found to be exempt under this provision includes:

- references to prison procedures
- compliance with prison order and rules
- details of prisoner movements; and
- prisoner supervision, security and safety procedures.

There may be crossover between this exemption and prejudice a procedure for protection a building and structure. For example, a prisoner or someone from outside a prison applied for the layout or plans of a specific prison. Depending on the way the application was phrased you might be looking at protection of a building, structure or vehicle or you might be looking at facilitate a person's escape from lawful custody; either could apply depending on what documents were brought back. I could see there definitely being some crossover between those provisions. If it was specific applications for prisons, prison layouts, prisoner transport vans or information about the locking mechanisms, prisoner transport procedures etc—depending on how the application was phrased it could be triggering 10(1)(j) as well as protecting the building, structure or vehicle. So there can definitely be crossover within these provisions depending on how the application is phrased.

Slide 15 (21:50)

10(1)(k) is the last provision in 10(1). To the best of my knowledge, it's never come to the Office of Information Commissioner on review. I'm going to cover it briefly because for all I know there's an agency out there that's running this all time and running it very well. 10(1)(k) is about the protection of a cultural or natural resources or plants or animal habitats. Information is exempt if its disclosure could reasonably be expected to:

- prejudice the wellbeing of a cultural or natural resource; or
- prejudice the wellbeing of the habitat of animals or plants.

Prejudice means to detrimentally impact. *Wellbeing* means good or satisfactory condition or existence; welfare.

Slide 16 (22:39)

The information must:

- concern a cultural or natural resource or a plant or animal habitat; and
- its disclosure must have a reasonable expectation of prejudicing its wellbeing.

Examples might include:

- draft environmental management guidelines
- management and zoning plans for protected wildlife areas

If an agency has got information that shows, for example Aboriginal or Torres Strait Islander cultural areas that are not open to the general public that would absolutely, definitely fit under this provision. I don't know if people are running this, I don't know if it's ever come up. I don't think anyone's ever called through the Enquiries Service asking about this provision. To the best of my knowledge it's never come on review; there are no decisions about it anyway. I just wanted to mention it and make people aware that it's there if it ever does come up. Because it's never come up I don't really have anything to say about it except for making you aware of its existence. Do be aware that it's there and if it does come up and you do think it does apply feel free to contact us and we can have a chat about how best to run it if you need to.

Slide 17 (24:05)

We touched 10(1)(2) way back at the beginning but I just wanted to briefly touch on 10(3). I don't know how often this comes up but again I just wanted to make you aware of it.

10(3) is a bit different from 10(1) – there's no reasonable expectation test attached to it. It's a straight question of fact. If X then Y. X in this case being: if the information that you're looking at was given under compulsion under an Act that abrogates the privilege against self-incrimination during an investigation into a contravention of the law, it is exempt. There's no question of, "and it's going to have X/Y/Z effect or there's a reasonable expectation that it will have X/Y/Z effect." It's a simple question of fact. If the information was, to use a privacy term, collected in this way it is exempt from release.

Slide 18 (25:20)

First of all let's talk about the privilege against self-incrimination. If you've ever watched any American crime drama you're probably familiar with the right not to incriminate yourself. Basically in Australia at common law you have the right not to incriminate yourself. That means that if you're asked a question and answering it would tend to incriminate yourself you don't have to answer it. So if someone says "did you see Johnny steal the painting?" and your answer is going to be "yes, I did see Johnny steal the painting" but the only way you could have seen Johnny steal the painting would be if you were right there with Johnny while he was stealing the painting that would tend to incriminate yourself with at least breaking and entering into wherever the painting was stored and possibly to painting stealing. I'm not an investigator or a criminal so I don't know the right terms there. At common law you could just shut up and not say anything.

Some Acts override this right not to incriminate yourself. They give investigators the power to compel you to answer questions even if the answer would tend to incriminate yourself. So, schedule 3, section 10(3) says that if the information that you, as a decision maker, are looking at was acquired that way it is exempt. But the things you have to determine as a decision maker are:

- was there an investigation into a contravention or possible contravention of the law on foot
- was this information collected/acquired as part of this investigation
- does a power like that exist in whatever Act gives the investigators power; and
- was it actually used?

Just because an investigator has the power to compel information from someone doesn't mean that they actually used it. So that's a very important step that you're going to have to take. You might have to do some digging to find that out. It's easy enough to go and look at the Act and see if it does have a power to compel information. If you have a look at the Law Enforcement guideline you will see we have an example in that Act and the wording that's used, so that's a decent guide for you, or you can call us, that's not a problem.

You can look at whether or not there was an investigation ongoing. That will be obvious from the file. Finding out whether the power was actually used, well, hopefully it will be on the file; some investigators may issue a notice to the witness. But if it's not obvious you're going to actually have to find that out. The information is only going to be exempt if the power was actually used to compel the provision of the information.

I'm probably spending more time on this than is warranted because I don't know how often it comes up. If there was a power and it was used during an investigation into a contravention or possible contravention of the law the information is exempt from release.

Slide 19 (28:45)

That's it! Well that's obviously not all of schedule 3, section 10 – there's the entire CCC exemption which as I said before would take an entire video in its own right. There's a few more bits and pieces floating around in schedule 3, section 10 which are covered in the guidelines and the annotated legislation and you can always contact us at the Enquiries Service if you want to have a chat about them generally or specifically and we will do our best to assist you. That is it for this video.