
# Education and Home Affairs Scrutiny Panel

# Camera Surveillance in Jersey Review

## WEDNESDAY, 26th JUNE 2013

**Panel:**

Connétable M.P.S. Le Troquer of St. Martin (Chairman)
Deputy M. Tadier of St. Brelade
Deputy G.P. Southern of St. Helier

**Witness:**

Data Protection Commissioner

[10:01]

**Connétable M.P.S. Le Troquer of St. Martin (Chairman):**

Welcome, everyone, to this public hearing this morning. It is in relation to the review that we are carrying out by the Education and Home Affairs Scrutiny Panel into the C.C.T.V. (closed-circuit television camera) surveillance on the Island. Can I just ask, please, Commissioner, how long have you been the Data Protection Commissioner?

**Data Protection Commissioner:**

In this official title, since 2005.

**The Connétable of St. Martin:**

Were you the first?

**Data Protection Commissioner:**

Yes, but I was the Registrar before, so slightly confusing, but in terms of Commissioner on this law, yes, 2005.

**The Connétable of St. Martin:**

I was going to say what sort of experience had you had as the Commissioner?

**Data Protection Commissioner:**

I was Registrar and Deputy Registrar before that, and then prior to that, I was the Data Protection Officer.

**The Connétable of St. Martin:**

Thank you very much. What sort of size is the department? It would be quite interesting to know.

**Data Protection Commissioner:**

As you may well know, we now look after Guernsey as well, and there are 3 of us in each office.

**The Connétable of St. Martin:**

Guernsey 3 and Jersey 3, including yourself?

**Data Protection Commissioner:**

Yes.

**The Connétable of St. Martin:**

But you are supervisor, if you like, then of Guernsey as well?

**Data Protection Commissioner:**

Yes, that is right.

**The Connétable of St. Martin:**

Could you outline the role, please, of the Data Protection Commissioner in relation to the uses of video surveillance cameras on the Island?

**Data Protection Commissioner:**

Video surveillance - and indeed photographic images - are data, in that they identify individuals potentially, and in the sense that they are data and identify a person, they are captured by the definitions of the Data Protection Law, which is a law that sets out the framework of control around how organisations handle and use personal information. So as they are used commercially and by States departments and by organisations, they are captured by the requirements of that law.

**The Connétable of St. Martin:**

What percentage of your time of your department do you think C.C.T.V. takes up, because you have lots of other responsibilities?

**Data Protection Commissioner:**

We do, and there is so much data around, an increasing amount of data around these days, so I cannot say that it takes up a great deal of our time, but as I mentioned in some of the comments to the panel, we have noticed - because we have all been working there for some years now, and so you get attuned to trends of inquiries - that in recent years there has been an increased number of general inquiries as opposed to official complaints. Now, official complaints are logged and there are a number of statistics that we can glean from those, but we also deal with a significant number of phone inquiries and walk-in inquiries and we have noticed, and it is anecdotal, as I have mentioned, that there increased concern. Now, one of the complexities of that point is that the Data Protection Law does not capture what is called domestic use C.C.T.V., so if you put up a C.C.T.V. camera on your property, you are not a business, you are not a States department, that it is just a home, then it would be exempted under the Data Protection Law. But we still get inquiries from neighbours, often warring neighbours, who are installing these cameras and upset their neighbours by doing so.

**The Connétable of St. Martin:**

We will come back to that a little bit later on, I think, into the private side of it. So the main regulatory controls that apply, can you go into that a little bit further? I mean, we know there is a Data Protection Act.

**Data Protection Commissioner:**

Yes. The law that came into force in 2005, it very much is in line with the European model of data protection and it applies the same standard. It does not differentiate between C.C.T.V. images and other data, so there are a number of rules that apply around the way in which data is collected. That is about transparency, it is about fairness of processing, the proportionality of processing, security of the data, retention of the data and access to the data. That is the broad framework of control that sits around C.C.T.V. images, as they do any other data.

**The Connétable of St. Martin:**
That control is where, in the Data Protection Act?

**Data Protection Commissioner:**
That is right. They are the data protection principles within the law itself that set out the framework of compliance requirements.

**The Connétable of St. Martin:** The code of practice?

**Data Protection Commissioner:**
The law allows the Commissioner's office to publish codes of practice in areas where there is clarity needed or there is an area of concern, and the C.C.T.V. was an area where we thought it would be worthwhile to publish the code of practice some years ago, because we saw an increase in both the use and the number of inquiries that were coming to us. So the code of practice is something that we are allowed to do under statute. It is not a statute in itself.

**The Connétable of St. Martin:**
The police, for instance, some time ago when P.A.C.E. (Police and Criminal Evidence Act) came in the U.K. (United Kingdom), Jersey had its own codes of practice, but they were not lawful, as such. Now I know it has changed, but would this be the same? If you do not comply with the code of practice, your code of practice ...

**Data Protection Commissioner:**
It would be very difficult to envisage a situation if you did not comply with the code of practice that you would be in compliance with the law, but the code of practice itself is not a statutory requirement.

**The Connétable of St. Martin:**
So it would not be an infraction?

**Data Protection Commissioner:**
It is empowered by the statute.

**The Connétable of St. Martin:**
I am sorry, I interrupted you. It was my fault. It would not be an infraction of the code of practice? The code of practice is there. If you do not comply with it, you might be breaching the data protection ...

**Data Protection Commissioner:**
You are very likely to be, yes.

**The Connétable of St. Martin:**
I see. Okay. You said the code of practice was made by your department. What year was that, please?

**Data Protection Commissioner:** It was not long after the law was implemented, so around 2005, 2006.

**The Connétable of St. Martin:**
Updated since then?

**Data Protection Commissioner:**
No.

**The Connétable of St. Martin:**
It has not been ...

**Data Protection Commissioner:**
The law is the same. The law has not changed in respect of ...

**The Connétable of St. Martin:**
The codes have not?

**Data Protection Commissioner:**
No, the code reflects the law and the law has not been changed since 2005.

**The Connétable of St. Martin:**
By the time I got a video player, there were D.V.D.s (digital video discs) and you just cannot keep up with the way the world changes, but you are ...

**Deputy M. Tadier:**
Betamax.

**Data Protection Commissioner:**
The technology may change, but the principles behind data handling have not.

**The Connétable of St. Martin:**

Okay, yes.

**Data Protection Commissioner:**

So I think you can give the compliance requirements out publicly about security of data, access to data, openness of processing. That applies, regardless of the method, the media used to collect the data, so what we try and do is supply good advice, good guidance, good documents that it would apply, because technology is changing so fast that we could not keep up if we just did it for iPhones or just for tablets or just for that specific type of processing. We have to do it in a broad brush way that covers all sorts of media.

**The Connétable of St. Martin:**

Okay. As I say, it is fair to say then the legal framework for the operation of video surveillance is determined by your office?

**Data Protection Commissioner:**

It is determined by the law and we regulate that law.

**The Connétable of St. Martin:**

Do you think there is a satisfactory level of regulation at the moment for the technology that is available?

**Data Protection Commissioner:**

Broadly, yes. I think in terms of the way that organisations and public sector and private sector, the rules that apply to the manner in which they collect visual images are fair and they apply to that data, as they do other data. Now, it does not mean there is not room for improvement and there is certainly a lot of discussion in Europe at the minute about how to improve the data protection controls, but I think the framework ensures transparency, accountability, all those good things, is a robust framework.

**Deputy M. Tadier:**

Michel, can I just go back to a couple of points? We appreciate that you do not have the hard and fast numbers of inquiries, apart from the complaints which are being logged, but can you give us an idea maybe of the proportion and also the number of the split, so, for example, what I mean by that is how many are inquiries by people domestically who want to set up cameras and how many are by people complaining that their neighbours might be snooping on them?

**Data Protection Commissioner:**

I do not recall very many of the former, i.e. neighbours asking, domestic use asking, but last month we had 6 calls in one day because a camera had been installed in an area. It was private, but it was an area of flats and the 6 other tenants were very aggrieved with one of the tenants putting up cameras. So we can get 6 in one day and then nothing for months, so it is quite hard, and it is very labour intensive for ...

**Deputy M. Tadier:**

Was that put up by the individual owner?

**Data Protection Commissioner:**

Yes.

**Deputy M. Tadier:**

In St. Brelade?

**Data Protection Commissioner:**

No.

**Deputy M. Tadier:**

No. Okay, that is fine.

**Data Protection Commissioner:**

But just to clarify on statistics, there comes a point where an office spends more time collecting statistics than it does doing its job and we cannot record statistics on the nature of inquiries. It is a small team, so I can discuss with my team: "What sort of areas are you seeing that are of concern?" so it is much more anecdotal and I cannot provide with the stats in respect of that.

**Deputy M. Tadier:**

No, that is understandable.

**Data Protection Commissioner:**

But I think it is still helpful for you as a panel to get feedback on that sort of experience.

**Deputy G.P. Southern:**

But anyway, the individual cases are not covered by ...

**Data Protection Commissioner:**

Exactly, exactly, and we have always tried to have an open door policy in respect of people's concerns on privacy and we will never say: "We do not cover that. We are not going to speak to you." We try and assist them about the best route to seek remedy or to assist, but there is no statutory basis for any regulatory involvement.

**The Connétable of St. Martin:**

The voluntary codes of practice then, are there different codes of practice? You have got the ones that you have issued, but if you are a private company or you are operating C.C.T.V. somewhere, maybe one of the larger supermarkets or something, if they have their codes of practice or should they be complying with yours?

**Data Protection Commissioner:**

They may well be implementing their own. A big firm - I do not want to use any names, but maybe a supermarket - may well have their own, but in terms of the statutory basis upon which we publish ours, they would not have that. It will be more an internal mechanism of control.

**The Connétable of St. Martin:**

So it could come from a major company from the U.K. or something ...

**Data Protection Commissioner:**

It could do, yes.

**The Connétable of St. Martin:**

... that just have their own codes, the U.K. code, but they should be complying with ...

**Data Protection Commissioner:**

We certainly see that quite a lot for U.K. companies that come over here, that they have their own, and that is one of the helpful aspects of having a law which is based on the U.K. Act, because our Data Protection Law in Jersey is very similar to the U.K. Act.

**The Connétable of St. Martin:**

Okay, so we have got codes of practice. How do you know the codes of practice - a person in your department, I should say - are being complied with? Do you test or is it just because of the results of complaints?

**Data Protection Commissioner:**

It is the same question you can put to any organisation that is responsible for oversight of a law, it is how far do you go in ensuring compliance. That, you have to have a strategic view on how your department functions in terms of the proactive nature of its education, the reactive nature of its enforcement arm, and again, with a very small team, largely it is reactive. We try and be as proactive as we can. You will see we are trying to get a response in the media about the police cameras, the body cameras that they are looking at doing. So we try and maintain the dialogue, which I think is incredibly important, in the public sphere about the nature of surveillance; States surveillance we are talking about as well as commercial surveillance. It is terribly important, from my perspective, that this is a very open discussion, that the public are aware of what is on the table and how it is being handled. So we have to balance very limited resources with the avenues that are available to us in terms of educating people, in terms of there is a requirement for data controller organisations that are handling personal data to notify with us. We have a public register, so we have already a relationship with organisations and we are very responsive to inquiries from them. Most organisations want to comply; very few do not. So if they make a mistake, sometimes that is a trigger for them to review their processes and to improve their processes. C.C.T.V. is an area where employers get caught out. They will capture things on those images and do things with the images that maybe they should not be doing and it prompts them to review their compliance. So there is a whole number of factors.

[10:15]

**The Connétable of St. Martin:**

What sort of thing? What do they do?

**Deputy G.P. Southern:**

Could you exemplify that?

**Data Protection Commissioner:**

When you notify with us about the processing of personal data, you have to specify a purpose. That is a requirement of law. For example, if you have got a shop and your purpose for the collecting of that C.C.T.V. data is the prevention and detection of crime, so specifically you have stated to us, you have applied in law to process that information to stop people from stealing clothes, for example, if you capture a staff member skiving off, that is not a crime. It is a contractual disciplinary issue, okay? It is not what you have notified us for, the purposes, okay, so there is a disparity there. So they should not be collecting images ... they can say those images are for monitoring staff, but they have to say that upfront. You cannot retrospectively say. The same for anything: if I collect information for a raffle, I cannot then sell it on to a double-glazing

company unless I have said upfront. That is one of the rules of data protection, you have to be very clear upfront what the processing is for.

**Deputy M. Tadier:**

So if we follow on from that example, a shopkeeper who ostensibly has set up a camera to prevent or to capture shoplifting and then finds that there has been a staff issue, is she or she allowed to use that footage then?

**Data Protection Commissioner:**

No, no.

**Deputy M. Tadier:**

No, but does that happen?

**Data Protection Commissioner:**

Unless it is a crime.

**Deputy M. Tadier:**

Does that happen?

**Data Protection Commissioner:**

Well, if they speak to us, it gets resolved, because they know that they should not be using those images because they have been collected unfairly.

**The Connétable of St. Martin:**

But would somebody smoking that should not have been smoking in the back of the warehouse or something, they are caught smoking and get dismissed, would they know that that C.C.T.V. camera was used for a different purpose?

**Data Protection Commissioner:**

If that has been the evidence produced to them, they would be aware, and we have had inquiries from employers and employees in respect of that. It is not an uncommon scenario, I have to say. So one of the requirements of the law is that you have got to be upfront about the purpose for your processing. You cannot change that midway through.

**Deputy M. Tadier:**

Can I take it one step back, because when you register with data protection notification, you can do that for different reasons, so we should be registered with you now, but do you have register separately to set up surveillance in your shop if you are already registered for ...

**Data Protection Commissioner:**

It is a separate purpose, but you can do it under your own notification. For example, we will have the schools, a lot of the schools now have C.C.T.V. so they will have it as part of their notification, it will specifically say C.C.T.V.

**Deputy M. Tadier:**

But are you obliged to register a new one if you want to set up a ...

**Data Protection Commissioner:**

Yes. If you are purely collecting the C.C.T.V. data, then yes, you would, if there is notification for one.

**Deputy M. Tadier:**

But even if you are already registered is what I mean.

**Data Protection Commissioner:**

You would add that to your ... you need to be absolutely clear within your notification that you are processing C.C.T.V. images. There is the separate line, as it were, of notification.

**Deputy M. Tadier:**

But what I am saying is if you add that at some point, you have already got your notification with the department, do you have to then come again to the department to say: "We are setting up a video camera"?

**Data Protection Commissioner:**

No, you just amend your current notification.

**Deputy M. Tadier:** Okay.

**The Connétable of St. Martin:**

How would you know if someone has not notified you or has not registered with you? You do not know? You would not know?

**Data Protection Commissioner:**

We do not know. How do the police know when someone is speeding at this point on Victoria Avenue? Unless you are there, unless you have another mechanism of control, you do not, so you have to be reactive on inquiries when new businesses are being set up. We work with financial services to make sure that businesses are given information about the legal requirements when they are setting up business, so if they are handling personal data, one of the checklists is to check with our office whether they need to be notified. So we do various things, but ultimately the answer is I do not know.

**The Connétable of St. Martin:**

You would not know. If somebody wants to start up a little business in the Island and they think they have covered every avenue, but they are going to have a C.C.T.V. in their shop and they have not registered with you, they would then be breaching the Data Protection Act?

**Data Protection Commissioner:**

If they are processing personal data and they are not notified and they are not covered by a small business exemption, which there are some, then they would be committing an offence, yes.

**Deputy G.P. Southern:**

You mentioned some principles earlier out about data handling. I just wondered if you could explain how they apply to C.C.T.V. images. You mentioned security.

**Data Protection Commissioner:**

Yes. That applies across all data, so that information, when I go to my doctor's surgery and she pulls out the notes, I do not expect them to be just left on the public counter when I am gone. It is not about high-tech rocket science, it is about practical, sensible security of data, whether that is my doctor's notes or whether it is images the police are taking. If they are taking images on the body camera, where do those images go, who has access to those images, where are they stored, how are they deleted? You know, all those questions apply, regardless of the nature of the data, but they apply equally to photographic images.

**Deputy G.P. Southern:**

So that one of about access. You mentioned transparency.

**Data Protection Commissioner:**

It goes back to the notification point, that you have got be clear with us what you are processing information for, but you have also got to be clear to the individual that you are collecting information from who you are and what you are going to do with their information. So when you

are filling in any form, any of us, whether it is online or offline, we should be clear about who we are giving our information to and what they propose to do with it. That applies with C.C.T.V. That is where you have seen signage in areas. You have seen the front of Morier House; there is C.C.T.V. in operation. That is about an openness in collection of data. This is not about covert surveillance. That is a very, very different beast. This is about overt processing and I think indeed the police would not want it to be covert, that sort of data collection, because that is part of the package, I think, is the deterrent factor.

**Deputy G.P. Southern:**

The other word I picked up on was "processing" was something you said that applied to this.

**Data Protection Commissioner:**

That is literally how the information is handled, so I keep going back to the police, but it is a good example, so how literally that is handled and how physically it gets transferred back to wherever it is being processed, so "process" is just a word for either physically handling data, you know, what happens to this piece of paper or electronically where it is going and who has access to it.

**Deputy G.P. Southern:**

So it does not go to You Tube and the police can ...

**Data Protection Commissioner:**

It is interesting, because if you look at the U.S. (United States) these images that the police collect get sold. They have whole TV programmes. We joke about it, but in a sense if you look at it in a more general sense, I feel quite lucky I am not in a jurisdiction that, you know, I have a car accident and it happens to be filmed by a police officer and the next minute it is on primetime ITV. So I think that is the reality of having a robust data protection framework, which we often forget about how it plays out in real life. But that is the stark difference between a jurisdiction that does not really have much privacy, statutory control, and an area that has.

**The Connétable of St. Martin:**

The showing of that footage, I mean not for television programmes, but trying to locate somebody, is that right, should it be shown on T.V. (television)? What rights ...

**Data Protection Commissioner:**

The same would apply to images. If they have got a mugshot at the minute, the same applies to that. It is just collected in a different way, so if it is for the purpose of policing, so if an incident were to happen - we are going back to the police example, I know - and the camera gets triggered and that offender leaves the scene and is not apprehended at that point, those images could be

used, could be, for public dissemination if it was for the prevention and detection of crime, so if that person was at large and a risk and wanted, then that image could be given to the media.

**The Connétable of St. Martin:**

That is how it is done now then? That is how it is given out?

**Data Protection Commissioner:**

Exactly the same just on that. It is not a free for all, it is not just: "Look at this particularly interesting arrest." There has to be a reason for the disclosure of that particular piece of information to the wider world.

**Deputy G.P. Southern:**

Before we move on, did I miss out any other principles maybe you want to mention?

**Data Protection Commissioner:**

Purpose limitation. That goes back to the T.V. thing, that they can collect it only for policing purposes. That is a really, really important one from my perspective, and that applies, you know, if you fill in a competition in the *J.E.P. (Jersey Evening Post)* and then they cannot then sell it on to whoever they like, unless you have consented to that. So the purpose limitation is a very important one and links back to the notification about C.C.T.V. and why you are notifying, that you cannot say you are collecting it for policing and then use it for disciplinary. You have got to step back and be clear about what you want it for.

**Deputy M. Tadier:**

How would anyone know in the case of an unfair dismissal, how would the employee know what the purpose of that footage or the camera was registered for?

**Data Protection Commissioner:**

There should be signage. It is slightly different when an employee is being monitored in their workstations, but there should be absolute clarity. We suggest, when we speak to H.R. (human resources) professionals, it is about being in handbooks, staff handbooks, staff training, they understand why they are being surveyed, what has happened to the images, there is integrity around those images. We had a case quite recently where somebody wanted to put cameras inside toilets in a workplace, and that is just a real chronic invasion of people's privacy, but they were concerned about ... I do not know, whatever they were concerned about. So there needs to be a dialogue with the staff, I think, to make it fair, so they understand what is the problem the employer is trying to address? Is it shoplifting, is it attendance? What is it? Once you understand what the problem is you can then take a view on whether the response is proportionate. If you do

not know what the problem is, how can you give a view on whether that response is proportionate? If you have not had any shoplifting, if there is no problem of shoplifting in Jersey - which sadly, there probably is - and you put cameras everywhere, what are you trying to do? What are you trying to remedy there? So there should be an openness with employees about the nature of the problem and the extent to which the employer is trying to deal with that problem, so they should know. They should be told: signage, handbooks, anywhere like that would be acceptable. But they should not be surveyed without being told. That is covert surveillance.

**The Connétable of St. Martin:**

I think you were going to talk about codes of practice generally, but I think quite a lot of the things we were going to talk about ...

**Deputy M. Tadier:**

I have got one more question about the storage and the periods of time. What is the standard accepted norm for storage of C.C.T.V. footage?

**Data Protection Commissioner:**

It very much depends on who is collecting it, because there is a world of difference between the local grocery store and the police, for example. The law is not specific. It talks about you hold it for as long as required for the purpose, so it links back to that purpose, so every organisation will have a different retention period. They should have a retention period. That will be largely based on their own expectations of use of that data, potential legal proceedings. For the police it will be slightly different, because an incident that happens today and the arrest and they are charged, it may be prolonged because of an appeal. They will want to retain that for quite some time, I would suggest, if it is in connection with an actual offence. For shops, it is probably less, and the more you hold, the more difficult it is to store, the more issues you have got about security, the more issues you have got about access, so while it is probably easier than ever in this world to keep data, it still raises the problems that were there historically about ensuring people have access and ensuring the storage is secure.

**The Connétable of St. Martin:**

If you passed on your data, if you are a shop and you are passing on to the police, where does the responsibility then go? Does it remain with the shop or does it then ...

**Data Protection Commissioner:**

The shop in the first instance is the data controller. That is the person in law who is responsible for the data. If they pass it to another data controller, i.e. the police, as long as they have done it in accordance with the law, which is if they have had theft in their premises, they pass it on for that

purpose after a request from the police or they put it to the police because they have had that theft, the police are a data controller in their own right. So if the police mishandle it, it is the police who are responsible, but if the first data controller has disclosed it inappropriately, they are responsible. So in a sense they are both responsible, but once the data has been given lawfully to the police, they are then responsible in law for that.

**Deputy G.P. Southern:**

I notice you said you did not feel the need to update your current practice to respond to ...

**Data Protection Commissioner:**

I think I said we have not.

**Deputy G.P. Southern:**

You have not.

**Data Protection Commissioner:**

Because the law has not changed. I would love the time to have a zappier website, to put a lot more stuff out there, but the reality is we are a very, very small team in an incredibly demanding area of law that is challenging us in all sorts of ways we did not think it would 5, 10 years ago. So yes, I think it probably could be better. There is not anything on my desk that could not be better, but it is about whether you have got the time, the money, the resources to do it. So yes, I think this is a good opportunity for us to review and take stock of this.

**Deputy G.P. Southern:**

In the light of the U.K. Surveillance Camera Commission has just published a new C.C.T.V. code of practice, I think that ...

**Data Protection Commissioner:**

Absolutely, we are very open to ...

**Deputy G.P. Southern:**

Are you working on that?

**Data Protection Commissioner:**

We are not, no, at the present time, but I think that we are in the middle of a huge review of data protection legislation in Europe which will impact Jersey. My priority at the minute is establishing how that is going to affect Jersey, because it is significant. It is probably the most significant thing

to happen in the field of data protection in many a year, if not since its birth. So we need to see how that is going to shape before we start tinkering with our own legislation or statutory controls.

**Deputy G.P. Southern:**
There is a bigger wave coming.

**Data Protection Commissioner:** Yes, a tsunami.

**Deputy G.P. Southern:** We will wade in the surf. Would you like to tell us more about what you see of the developments and what you are expecting? Are we at that stage yet?

**Data Protection Commissioner:**
In terms of?

**Deputy G.P. Southern:**
In the terms of the European changes.

**Data Protection Commissioner:**
So wider. For anyone that follows the interest that the Commission have in data protection, it largely centres around what they call the right to be forgotten, which is trying to address, especially the younger generations, the digital trail that they leave. I was at a talk that was given yesterday to a bunch of very, very young children. I do not think there was not a hand that did not go up - these were 8 and 9 year-olds - when asked: "Are you on Facebook and are you playing 18 plus games on PlayStation, Xbox, that sort of thing?" Staggering. So these children are online for hours on end in an adult world and they are leaving a trail, and as they grow up, that trail just gets bigger and bigger and bigger.

[10:30]

Again, in our office we have a noticeable number of young people, young adults, who are now reaping, they are not positive rewards, they are negative rewards, because of things they did when they were 16, 17, photographs they put up or their friends put up come back to haunt them, because employers do do searches; regardless of references, regardless of qualifications, they will do internet searches. So the European Commission is very concerned about the impact that will have, especially on the younger generation as they grow up. So there is a desire to empower people to be able to remove some of that information and have a statutory basis for its removal. So that is probably one of the most significant things in terms of individual rights. In terms of regulators, at the present time if a Jersey resident signs up to an Indian company for a product and

that Indian company misuses their personal data, there is not a lot I can do. What this new regime will look like, it is called geographic-based rights. Regardless of where the data controller is, so where the company is that I am dealing with, because I am in Jersey, I am afforded those rights, which is again a huge leap forward. So there a whole host of others. I could speak for days on it, which I will not bore you with, but it is big, and it is trying to recognise that in the 1980s, which is when all of this law was drafted, the world was very, very different technologically speaking. I go back, because I think the principal thing to say is the same, about transparency, accountability, access, all that needs to stay the same, but the language needs to maybe be updated to reflect the way in which we are ... I will call it datafication, things that were never sitting in data form are now in data form: who I like, if I am on Facebook, who I do not like, who I am chatting to, things that were ephemeral before are now permanent and it is how we deal with that. I digressed slightly in answer to your question.

**Deputy G.P. Southern:**

I think it is wider. When you talked about transparency before, you mentioned, okay, there is a sign outside Morier House. I understand that the general police surveillance cameras are not signalled. Is that something that ...

**Data Protection Commissioner:**

We would expect reasonable efforts. Now, in Morier House, in this building, it is not difficult. They only come in one door, they go out one door. I can see the signage very clearly. The police, the law enforcement cameras are everything, and you cannot have signage - I do not suppose Planning would be very happy - on every single area of the town or the roads that are covered, so they are very, very obvious, they are huge great ...

**Deputy G.P. Southern:**

I do not think they are that obvious though, to be fair, because you are not walking around with your ... until this review, I did not know where any of the cameras were.

**Data Protection Commissioner:**

Yes, once you start looking, you notice, do you not?

**Deputy G.P. Southern:**

Yes.

**Data Protection Commissioner:**

There is no attempt to hide them.

**Deputy G.P. Southern:**

In the absence of putting signs up, what other steps could the police reasonably take to inform the public of the locations?

**Data Protection Commissioner:**

I suppose if you made an equivalent of an F.O.I. (Freedom of Information) request, they will give you the location of the overt cameras. I do not know. I have not tried it.

**Deputy G.P. Southern:**

What about an online map of where the cameras are?

**Data Protection Commissioner:**

Possibly, yes, yes.

**The Connétable of St. Martin:**

Then why should it just be restricted to the police, because the private companies ...

**Deputy M. Tadier:**

I do not think it is.

**The Connétable of St. Martin:**

That is right, it is not, is not? But if the police ...

**Data Protection Commissioner:**

I think the difference is that for the police that it captures a lot more of our daily lives and I think if it is just one particular shot, the potential for a privacy intrusion is different than it is if the police have access to it. They could follow me basically from driving along Victoria Avenue, turning off Gloucester, parking, walking to work. They have potentially ...

**The Connétable of St. Martin:**

It is part of the training, yes, to follow a person.

**Data Protection Commissioner:**

Yes, certainly a way that the spa shop would not, you see? They would capture a moment in time, but not that broad spectrum of behaviour that would be demonstrated if you can follow somebody using a plethora of cameras.

**Deputy M. Tadier:**

I was going to ask, just to clarify - and I am sorry if I have not understood it - but does anybody, whether it is a government body or a private individual, need to seek permission from your department to set a camera up, or it is simply they need to notify you?

**Data Protection Commissioner:**

There is what is called a domestic use exemption, so if it is for my own personal use for any data, if I have just got a laptop at home with a Christmas card list on it, I do not have to notify the data protection authority. The same applies for C.C.T.V. The difficulty with that, and I think you are probably coming on to the personal use later, is that it impacts on other people, whereas my Christmas card list at home would not. But if I put a camera outside which is zoomed on to the neighbour's back garden, it has the potential to impact that person. I think there is a difference.

**Deputy M. Tadier:**

If we take the shop example, if I am a shopkeeper and I say: "I want to have a camera for X purpose" and I tell your department, how does that work? Can you stop the shop having a camera?

**Data Protection Commissioner:**

No, no. It is not illegal.

**Deputy M. Tadier:**

It is not illegal?

**Data Protection Commissioner:**

To process data without being notified is illegal, so all we could require of them if they did not notify with us is for them to notify with us. But they do have to abide by other principles, which is about transparency and fairness and security, so all those requirements apply whether or not they are notified.

**Deputy M. Tadier:**

What happens if they do not?

**Data Protection Commissioner:**

Well, we receive a complaint usually. I mean, we do not go around testing these things. We have done a few audits in our time, but they are incredibly time-consuming, but usually we are responsive in terms of complaints about breaches of principles, so somebody will say to us ... we had a query the other day that there was a garage with no signage, so we will contact them and

say: “We have had an inquiry [on a no-names basis]. Do you have C.C.T.V.? Do you know you need to be notified and do you know you need signage?” and 99.9 times out of 100 they will say: “Oh, did not realise” so there is an education thing here which we take on board, but it is also that our job is just to remind people, and in a pragmatic way, not to go in with size 15s and say: “We are going to take you to court for not notifying.” Clearly, if they refused we would do, because it is an offence.

**Deputy M. Tadier:**

But the signage, for example, is that a requirement of the law or it just ...

**Data Protection Commissioner:**

The requirement of the law is that you are fair about how you handle information and you tell people what you are doing and why you are doing it. It is slightly more difficult with C.C.T.V., because if you are filling in, registering in for a doctor, they should be clear about what they are doing. It is quite easy to get you to sign up to that, but when it is surveillance, it is subtlety different and that is where you will see differences in approach. But certainly our view in the code is that you should make every effort to inform people if they are in an area that is covered by C.C.T.V.

**Deputy G.P. Southern:**

The notification process, in that, you would be talking to them about what is a reasonable length of time to store, access et cetera?

**Data Protection Commissioner:**

Yes, absolutely.

**Deputy G.P. Southern:**

That would be checked out, would it?

**Data Protection Commissioner:**

A lot of our time is spent advising data controllers.

**The Connétable of St. Martin:**

Do you know how many C.C.T.V. cameras that are States owned operating today?

**Data Protection Commissioner:**

No.

**The Connétable of St. Martin:**

You do not. Private shops?

**Data Protection Commissioner:**

No.

**The Connétable of St. Martin:**

Do not know, so there could be thousands?

**Deputy G.P. Southern:**

Do you know how many have been identified?

**Data Protection Commissioner:**

Yes. I do not have it here now, but I could, yes.

**The Connétable of St. Martin:**

So there could be thousands?

**Data Protection Commissioner:**

I am confident in saying that there are many more than are notified with us, but there are also many, many personal cameras out there as well which do not need to be notified.

**The Connétable of St. Martin:**

Or controlled. Well, yes, if they use the information, if someone had a private ...

**Data Protection Commissioner:**

They are exempted from the law.

**The Connétable of St. Martin:**

They are exempted totally. Have there been any convictions for breaching the data protection in relation to cameras?

**Data Protection Commissioner:**

No.

**The Connétable of St. Martin:**

There have been no convictions?

**Data Protection Commissioner:**

But do not forget the principles, there are the principles that the Deputy spoke about are regulatory. There is a 2-pronged approach to breaches in the Data Protection Law. One is

regulatory, for breach of the principles, and there we issue what is called notices, and there is the criminal, and the criminal, there are very few criminal offences in the Data Protection Law. One is failing to notify and one is taking data that is not yours and selling it or doing something that you do not have authority to do, so for C.C.T.V. purposes, you are looking at a breach of principles, so you would not be looking at offences necessarily. I mean, you might be if someone was not notified and had refused to notify, but that has not happened.

**The Connétable of St. Martin:**

So that is statutory nuisances, and environmental people, they will issue an abatement order or something. You would be the same sort of thing, would you?

**Data Protection Commissioner:**

Yes, very similar, very similar, regulatory notice, yes.

**The Connétable of St. Martin:**

Just giving advice on what they have to do?

**Data Protection Commissioner:**

It is setting out of what the problem has been, where the breach has been and setting out the requirements that our office has for them to respond to that or rectify it.

**The Connétable of St. Martin:**

Thank you.

**Deputy G.P. Southern:**

Do States departments come to you when they are setting anything up? Do you know? They are particularly good at noting ...

**Data Protection Commissioner:**

I cannot say confidently that they all do, but because they are sort of a captive market for us, they cannot really escape: we know where they are, we know who they are, we know exactly what they are doing in terms of cameras; they tell us. So we are very proactive and I have to say I am of the view that because interaction with the public service is very infrequently voluntary that there is a higher standard that should apply, so I do not make any apology for spending a bit more time on compliance at Government level, because I think it is terribly important, and especially law enforcement level, because it matters. It matters for a whole host of reasons, but it certainly does matter.

**Deputy M. Tadier:**

I am sorry to labour this point. I am just trying to understand the limits of the code, and let us imagine there was a rogue employer who had set up cameras and they were using it, for example, they were doing audio recording of the public and they were spying on their staff when they were not supposed to be doing that and they were keeping the data longer than they needed to. Under law, what could your department do to prevent them?

**Data Protection Commissioner:**

In the particular case, there would a prosecution for failing to notify. There would be a notice to delete the data, so the remedy, there are things that can be done.

**Deputy M. Tadier:**

Imagine they had notified though, they had already notified you.

**Data Protection Commissioner:**

They will be regulatory breaches.

**Deputy M. Tadier:**

They are reportable?

**Data Protection Commissioner:**

Yes.

**Deputy M. Tadier:**

So, for example, it says in the code that it seems to be advisory how long they can keep data for.

**Data Protection Commissioner:**

The retention period is a difficult one and organisations frequently come to us to say: "Can we have a retention schedule for our business?" The law was never designed to be that prescriptive. It is linked to the purpose, so I have sat with organisations and they have said: "Well, we keep it for 20 years" whatever, and I will say: "Why?" The one question I put back to people all the time is: "Why?" and if the end of that dialogue: "Just because we always have" or: "Do not really know" the answer should be: "Well, as the statute of limitations, broadly speaking, which we consider to be around 3, 5 years." We hold it for 2 further years to ensure that if there is any latecomer in terms of legal action, then we have got the data covered. That is the sort of response I want, not: "Just because we can." Again, going back to the question of storage, it is so easy to store vast amounts of data. It is too easy just to say: "Because we can." You need to have a reason and if you do not have a reason, you should not be holding it. So we put that question back to organisations all the

time on these questions of retention. In terms of some activity that the Government does, it is useful for them to hold it for historical research purposes, so again, there are carve-outs in law for that, but you have got to be clear. You cannot just say: "Well, we do not really know, but we just put it in that room in disc form until the room burns down" or whatever. That is not a good enough answer.

**Deputy G.P. Southern:**
So it is a combination of purpose and what is reasonable?

**Data Protection Commissioner:**
Yes.

**Deputy G.P. Southern:**
Is there any regulation around what the signage should be?

**Data Protection Commissioner:**
No, in a word. It is about clarity of what is happening and who it is doing it. I notice when I go to the U.K., they have contact numbers a lot more than they do over here, so it is just an interesting observation.

**Deputy G.P. Southern:**
So who is the operator there? Is there ...?

**Data Protection Commissioner:**
Yes, exactly, if you have got any queries. It is probably less of a problem in Jersey to identify who it is, because if you go into Sand Street you know who to go to if you have got a query on that. In a way in the U.K. it is more anonymous, there is sort of a huge collection of data going on all the time in all sorts of areas. It is probably more difficult for the individual to establish a link with that data controller than it is over here, so I do not feel overly-exercised by the lack of a contact number, because I do think that if someone comes to us and says: "Listen, I think this camera is doing what it should not be doing or it is in a place it should not be" we would be very proactive in that respect. So yes, I think it can be improved, but I do not think it is a huge area of concern, the signage.

**Deputy G.P. Southern:**
Because again, and I am not going to go into detail, a log of visitors for a C.C.T.V. control room. Would you expect that or would you expect them...?

**Data Protection Commissioner:**

For law enforcement? A C.C.T.V. control room is something ...

**Deputy G.P. Southern:**

Anybody operating a control room.

**Data Protection Commissioner:**

That is someone with a lot of money, I would say. That is either the States or it is a private company with a lot of valuable stuff, you know, a large bank or something. For law enforcement, yes, I think there should be an audit trail in the way that for any sensitive data, there should be an audit trail of who has accessed it and why. If we have an inquiry about a health record, there should be clarity about who ... I should be able to know who has been looking at my health files.

**Deputy G.P. Southern:**

Who has access to it would be part of the process ...

**The Connétable of St. Martin:**

If we go and have a look as a panel at police H.Q. (headquarters) we should be recorded somewhere?

**Data Protection Commissioner:**

I would expect you to at least have signed in at the front desk and then there should be some reference to your visit made, yes.

**The Connétable of St. Martin:**

Sorry, Geoff.

**Deputy G.P. Southern:**

It is okay, I have cleared out my little list of things you might want to regulate. The requirement for training for C.C.T.V. handling, is that ...

**Data Protection Commissioner:**

A legal requirement?

**Deputy G.P. Southern:**

Yes.

**Data Protection Commissioner:**
Or what our expectations would be as regulator?

**Deputy G.P. Southern:**
Should there be?

[10:45]

**Data Protection Commissioner:**
Again, you are dealing with such a wide variety of potential images here, you are dealing with a corner shop, it is not going to be handling what would potentially be hugely sensitive information, as opposed to law enforcement. We keep coming back to them, but I know they were an important trigger factor in this review. Training would be absolutely crucial and it would be part of a response from us in terms of asking questions of them if there were a complaint, so we would ask what their policies are, we would ask what training is put in place for those who have access and process that data and we would ask all those questions. So yes, the greater the sensitivity of data, the greater the potential damage the data has on the individual, the greater resource and effort should be put in making sure the people around that process are properly trained and properly monitored themselves as well in terms of conduct. Who watches the watchers?

**Deputy G.P. Southern:**
That might be the next question. In general terms - and I think you may well have touched on this already - a register of C.C.T.V. systems to be held centrally, is that something that might be useful? What would its function be? Would you like to know how many cameras there are?

**Data Protection Commissioner:**
Yes, because it is data, and in theory the law, as it stands, should give us some idea of that. Because when the law was drafted there were a number of small business exemptions, we do not have a full picture of everyone processing personal data. I think it would depend what the objective was, because you can very easily see the objective starting out as just useful to know to becoming sort of a crime map, where to go if you do not want to be surveyed, if it is made public, so you have got to be quite careful of unintended consequences. You have got to be clear about your objective and make sure the audience is suited to that objective. But I am certainly open to consideration of a better mechanism for recording of surveillance cameras, yes.

**Deputy M. Tadier:**
You talked to us about that small business exemption. Is that still in place?

**Data Protection Commissioner:**
Yes.

**Deputy M. Tadier:**
How does that work?

**Data Protection Commissioner:**
If you are a very small business, it would not apply to C.C.T.V. images, but if you are a window cleaner and you do not have any offices, you do not have any real staff to speak of, but you just know Emma Martins owes you £20 and you keep a note, then that would be exempt from notification, not from compliance. You still have to look after the data. It is Government's way of saying: "Listen, we recognise this is going to cost you yearly. We do not want to penalise small business in an area which is a way of getting money in for the Government to run the regulatory regime" which is what it is. You do not want to overburden small business, so it was a recognition of that when the law was drafted.

**Deputy M. Tadier:**
But that does not apply to surveillance?

**Data Protection Commissioner:**
It would not apply to CCTV, no. But interestingly, some organisations that we have had queries about in the past, they are not live cameras, they are fake cameras.

**Deputy M. Tadier:**
Yes, dummies.

**Data Protection Commissioner:**
Cameras, yes, so ...

**Deputy M. Tadier:**
Have you got an opinion on the use of dummy cameras?

**Data Protection Commissioner:**
Well, technically I cannot have an opinion if they are not collecting data.

**Deputy M. Tadier:**
Yes.

**Data Protection Commissioner:**

I have an opinion.

**Deputy M. Tadier:**

Does it give a false impression though perhaps? I mean, it is perhaps not your area.

**Data Protection Commissioner:**

That is more a social question, is it not, about the impacts surveillance has on an individual, but the legal response to that is they are not collecting data, they are not captured by the law.

**Deputy G.P. Southern:**

With the advances in technology, so that we have now got highly-sensitive cameras that have got face recognition at a considerable distance, is that an area that causes you any concern?

**Data Protection Commissioner:**

Any data causes me concern in the sense that I want to see the law applied. If the law is applied as technology advances, it should do so properly. That is about being clear about the objectives, it is about being open about the manner in which the processing is happening, all those things we have already spoken about. So facial recognition: if I have got someone who looks uncannily like me, it is a false positive or a false negative. We have got to be clear that there is a system I am not automatically assumed guilty or innocent; it can go both ways. There has got to be a robust process of quality control in that. It does not take too much of an imagination leap to see where that could go when mistakes are made. So I think we have to accept that technology will race ahead. My concern has always been that we end up in a place where we have not decided we want to be, that technology drives us rather than us as human beings and our objectives, about how we want to see our society. That risks sounding trite, but you understand the point is that just because we can, we do. I think that is a mistake. I think we are at risk of going that way, more broadly, not just Jersey, generally. We need to just take stock and say: "What do we want? What are the issues? Why are we surveying? What are the problems? What are we seeking to remedy in surveying?" and then we can start a proper dialogue, but if we just do it because the cameras are getting cheaper, it is getting easier, the storage is no problem, let us just do it, that is where the danger lies, in my view.

**Deputy G.P. Southern:**

It comes back to this notification: what is the purpose?

**Data Protection Commissioner:**

It is all linked like a big jigsaw, all that, but I think more broadly there is almost a philosophical question here about the very nature of what we are doing and why we are doing it and we need to get back a little bit, especially in the question of surveillance, I think.

**Deputy M. Tadier:**

Can I ask, it kind of follows on - and I am sorry if I am jumping the gun here - and just move on slightly to the next section about access to official footage, let us say States footage. We are often told of its benefits for not so much crime prevention, but for prosecution. It is very beneficial because you have got factual evidence you cannot really dispute very easily. But is there a presumption that it can be used for defence purposes as well?

**Data Protection Commissioner:**

Sorry, States footage? Can you clarify?

**Deputy M. Tadier:**

Can it be used for defence, for example ...

**Data Protection Commissioner:**

When you say “States footage” what do you mean?

**Deputy M. Tadier:**

I just mean official police footage, for example.

**Data Protection Commissioner:**

Oh, police footage. Sorry, I thought you meant States footage.

**Deputy M. Tadier:**

Yes, States footage I mean, yes.

**Data Protection Commissioner:**

State owned, law enforcement footage.

**Deputy M. Tadier:**

That is it.

**Data Protection Commissioner:**

Sorry, carry on. Yes.

**Deputy M. Tadier:**

Yes, so is there a presumption of access for somebody to actually defend themselves, saying that they have been accused of a particular crime and ...

**Data Protection Commissioner:**

If that is evidence that is put for the prosecution, the defence are entitled to it as well, so yes, unless the provision of that data would prejudice that investigation or that case, the data should be given. It is complicated with C.C.T.V. because all sorts of other people are involved. It is never just Emma Martins walking down King Street, it is other people, and that in practical terms, the redaction of that data to remove third parties, if I happened to be in the background of a criminal act, I still have rights. I am innocent, I just happened to be walking past, so my rights should be protected as well. So it can be quite complex technically to properly redact those images, but the principal answer to that is yes, absolutely, I have rights of access to that.

**The Connétable of St. Martin:**

If I take it on further from the Deputy then, if you get a lawyer to defend you, the lawyer is going to expect to see that.

**Data Protection Commissioner:**

That will be full disclosure. That is a complete different thing, yes.

**The Connétable of St. Martin:**

Yes, disclosure, but if I am the member of the public and I am the defendant, if you like, the accused, and I am not aware that there is something on C.C.T.V., how do I know? Do I ask to see it? Do I ask?

**Data Protection Commissioner:**

Well, that should form part of disclosure. I know this is slightly off track, but if they are using that as evidence, if the police are using that as evidence, they cannot withhold that.

**The Connétable of St. Martin:**

If they are not using it as evidence, it might prove a person's innocence.

**Deputy G.P. Southern:**

Was not there, yes.

**Data Protection Commissioner:**

Oh, I see. I am with you.

**The Connétable of St. Martin:**

"I was not there" or: "I did not do what you are saying I am doing" and I do not know it is on camera.

**Data Protection Commissioner:**

If the defendant has got a good lawyer and they say: "I was outside Morier House or in the hallway of Morier House when the alleged incident happened. I know there is cameras there" that is a good lawyer's job, really. I am not sure I can add much more to that.

**The Connétable of St. Martin:**

Yes, it is just the member of the public who might not have a lawyer, who is not aware that there might be something that would clearly ...

**Data Protection Commissioner:**

I would like to think there is enough ... you know, if somebody goes to Citizen's Advice - we work a lot with Citizen's Advice - all the areas where there are flags against queries, and they come in and I get 4 or 5, 6 calls a week from those organisations, referred from those organisations. So of course that does not answer your question categorically, but if somebody were to seek advice, did not have legal advice and it involved the question of C.C.T.V. surveillance, they should be directed to us and we can at least give them the right tools to get access to those images, if they exist.

**The Connétable of St. Martin:**

They are entitled to see that without a lawyer from the police?

**Data Protection Commissioner:**

They are entitled to access data that is held about them, whether that is the road traffic report written by a police officer if they have had a crash or whether it is C.C.T.V. images. Clearly if I am being surveyed because they think I am committing a crime, they are not going to disclose that to me while that investigation is ongoing. So there are carve-outs to this. There are exemptions to that, because that would prejudice the investigation, but all being equal, if I have done nothing wrong, if I am not under investigation but I want it for civil purposes - I do not know, another reason - then I am entitled. If they have got information about me, then I am entitled to it.

**The Connétable of St. Martin:**

Back to you, sorry.

**Deputy M. Tadier:**

I guess the example I am talking about, imagine you have got an assault case outside a nightclub and there is an allegation of police brutality which the lawyer wants to make then. Have they got automatic access to the footage which the police would not necessarily bring it forward? They might say: "Right, we are going to use this 2 minutes of footage which shows the defendant attacking somebody else" or attacking the policeman, but they want access to 2 minutes before, where the policeman may have been attacking the defendant. How do the dynamics work for that?

**Data Protection Commissioner:**

That is more complicated because we often ... I often have to put the point to people that the subject access route under data protection, which is the right to see your own information, is not suitable for legal purposes, because it automatically has to consider third parties. Now, if I have been involved in an assault outside a nightclub, the interaction with third parties is absolutely crucial. My behaviour on its own may not enlighten anybody as to what happened that night, but so and so doing something else in the corner of that image or over there to provoke it or whatever it was, so it is called disclosure, full disclosure in terms of criminal proceedings. It is a legal route and it does not need to worry about third parties, so they would have the whole image. So I would discourage people from using the Data Protection Law as a route for any legal proceedings, because it only gives them a small amount. The same for this is a report about me allegedly assaulting somebody and I want to see my data. Say there were 3 people involved, I will just get my bits, so if I am taking this case forward, I need to know what John Smith did as well as what I did. So the fact that John Smith's data has been taken out means this report is useless to me in terms of legal proceedings. It can be the trigger. It can say: "Well, at least I know that I was seen there, because I was too drunk to remember" or whatever I was: "I know this is about me. I can now go to a lawyer and ask them for disclosure" which is the whole package. Does that make sense?

**The Connétable of St. Martin:**

You are done with citizens at the moment or do you want to carry on with that one?

**Deputy M. Tadier:**

Are we all right with that? Yes, okay.

**The Connétable of St. Martin:**

I think we have covered the codes pretty fully and now time is pressing on, so ...

**Deputy M. Tadier:**

But this does follow on largely from the rights of the citizens. Can you set out the rights of citizens and employees in relation to accessing camera footage?

**Data Protection Commissioner:**

It is a right that applies to all data. If an organisation holds personal data about you, you have a right to know what they are holding, and in most instances to copies of that data. It is called subject access rights and we get a lot more queries about that now than we used to. People are using that route for all sorts of data, not just images, and I know the police are much more geared up now to respond to requests for C.C.T.V. images these days, because as I said before, the practical challenges of pixelating or redacting third parties is quite tough.

**Deputy M. Tadier:**

So what about the practical difficulties, because I am sure if I turned up to the police headquarters and said: "I want all the footage you have got of me for the last 3 months" and then ...

**Data Protection Commissioner:**

You could not do that because you have to be specific, so if there was an incident ...

**Deputy M. Tadier:**

But they do not have to be specific when they are filming you, do they? They do not have to ...

**Data Protection Commissioner:**

No, they do not, but this is purely a practical administration route for you to get access to data you need, because unless something happened with you walking around King Street, your data will not be extracted, it will just sit. That is really important, because it is the implications of the processing in terms of privacy, which is terribly ... if every time your face hit a camera something else was triggered, that is where it becomes important, but if it just sits and if nothing happens, if there is no incident, it then gets deleted or archived and it is secure. The impact on you is minimal, if any at all. It is still sitting there, but if something else is triggered, so you are right, they do not have to be specific, but they are not doing anything specific to you in return. But if you want the data, the same with any information, if you just write to a huge organisation and say: "I want everything" they might come back and say: "Well, can you let us know what you want and when that email was sent?" or whatever, just to help them locate it.

**Deputy M. Tadier:**

But that is not the case for other types of data necessarily. If they have got stuff which is easily compilable then ...

**Data Protection Commissioner:**
Oh, if it is easily compilable, I mean, if it is my H.R. file sitting across the road, then they do not have to come back and say: “Can you be more specific?”

[11:00]

Yes, it depends on ...

**Deputy M. Tadier:**
Do you think that might change with facial recognition, if they have got different ways of storing ...

**Data Protection Commissioner:**
Again, it depends on what it triggers. If it triggers something, if you are wanted and it is something that is triggered every time your face comes up on those cameras, then the outcome of that, it is going to be relating to an investigation, let us be clear about that, is it not, on the whole? You will have access to that once that investigation is concluded, unless it is used as evidence. There are all sorts of different pathways that could go, but in theory, absolutely, yes.

**Deputy M. Tadier:**
How do citizens or employees know who to contact about their access to that information?

**Data Protection Commissioner:**
Employees need to contact their employer as the data controller. Citizens, that is why it is helpful to have signage, but if they are walking past de Gruchys and there is a camera there, they are going to know the data controller is de Gruchys. I have not myself ever received a query from someone who does not know who the camera belongs to. By virtue of its location, it becomes pretty clear, I think.

**Deputy M. Tadier:**
Do you think the public are generally well-informed enough about their rights in relation to surveillance or is there anything else we could do?

**Data Protection Commissioner:**
Their rights in terms of how the data was handled or rights of access or all of that?

**Deputy M. Tadier:**
I think probably all of that.

**Data Protection Commissioner:**

It is a good question. We have done some work over the years to raise awareness of data protection. We do as much as can we with the resources we have to help both data controllers and individuals. But, I said before and I will say it again, we can always do more and I think the difficulty that I have seen in practical terms when I first started in the role, we were very proactive and spent a lot of time going out and talking to people, making sure people were aware of their rights. We are now reaping the rewards of that in that the complaints, the inquiries are just deluging us. So in a sense the more proactive stuff you do, you have to be ready for the reactive stuff that results. So we go in cyclical periods in our office but I would always embrace any opportunity to improve people's understanding and awareness at an individual level, but also improve that at organisational level. Because I think, as I said before, most people want to do the right and they see data protection and think: "It is hideous, I cannot possibly do it" but it is about if it is your information how do you want it handled, just in a pragmatic sense, to be fair to you. That is largely what we are talking about here. There is not a lot in the law that is absolutely outrageous when it comes down to it. But, yes, awareness is a very important part and we could do more.

**Deputy M. Tadier:**

I suppose the political question is, is your department sufficiently well staffed to be able to meet that need?

**Data Protection Commissioner:**

I challenge you to put any public servant in front of your panel who would answer that other than: "Yes, we need more resources." Of course I could fill at least another 2 full-time posts easily with work but the taxpayer funds us, we are very mindful of that. We do work on very limited resources but everybody has to. The money does not come out of nowhere. So we are what we were created by the States and I am clear, when I am asked why I am not doing certain things: "Why are you not improving your code, why are you not updating this?" The answer is an honest one. If the States want more they have to provide us with the resources because not only are we doing Guernsey now as well, with no increase in resources, we are also dealing with a dramatic increase in concerns, queries about processing, because we are living in a new internet era.

**Deputy M. Tadier:**

I guess the question is whether you are optimally resourced. That may put you in an awkward position so I will not ask that question.

**The Connétable of St. Martin:**

I would put to you as well, without putting you in the position, same wording, you are just doing fire service policing in effect, that when you get a complaint ...

**Data Protection Commissioner:**

No, I would dispute that. We are not. The percentage of proactive versus reactive has shifted dramatically but that is not to say we do not do any proactive. Last week between myself and the Deputy Commissioner we spoke at 3 events. These are audit people, these are compliance people, these are members of the public. So we still do that. We still deal with inquiries, proactive inquiries, we still go out and help organisations with their compliance queries so while that percentage has shifted it is certainly not zero in terms of our proactive work.

**Deputy G.P. Southern:**

In fact you could say that it is a response to your ...

**Data Protection Commissioner:**

Well it absolutely is. I knew it would happen.

**The Connétable of St. Martin:**

With all the work that you have and you could do with extra 2 member and you would be updating, as you said, your codes or you would be proactive ... somebody would be out, we still manage to support Guernsey.

**Data Protection Commissioner:**

Yes. We have got F.O.I. around the corner as well.

**The Connétable of St. Martin:**

Sorry?

**Data Protection Commissioner:**

We have F.O.I., freedom of information, around the corner, which will be given to us as well. But we will ... the budget has not been finalised for that but we will have to have ... there comes a point when as a manager of an organisation you say you just could not cope. We would not cope without additional resources for F.O.I.

**The Connétable of St. Martin:**

I was going to ask a little bit later on but this maybe the time at this point. I know you said - I am positive the *J.E.P.* reported it correctly - that you are pleased that this review is taking place.

**Data Protection Commissioner:**

Very much.

**The Connétable of St. Martin:**

What do you think you would like to see come out of the review?

**Data Protection Commissioner:**

The first part of my answer will be that any discussion, open public discussion about the relationship between the state and the citizen, because this was prompted by the police cameras, is incredibly healthy and we should never forget that. We are very fortunate that we live in a jurisdiction where this is encouraged, so I like that aspect of it. I am frustrated a little bit by our inability to help the number of people that are increasingly coming to us with concerns. That is not to say that I think it may ... it needs to sit with us in terms of domestic use, but I think it is incredibly important that when publicly funded organisations like ourselves notice a shift in the nature of concern with members of the public, that that is somehow articulated through the political channels. That is the second part of the answer.

**Deputy M. Tadier:**

Does that happen and is that sufficiently ... the channel open there sufficiently well?

**Data Protection Commissioner:**

Well, this is it for me. I mean, we are independent and it is terribly important that we are independent because we oversee processing of the police, of States departments, so we cannot be linked, but sometimes that does cut off political routes for support and I do sometimes feel that. It is, in a sense, possibly just the natural consequence of being completely independent. But to have political interest in what is often seen as a very dry area, a not very interesting area, is terribly important for me and my team because we know we are dealing with people's lives. We know we are dealing with issues that affect people's lives. So I cannot solve those problems for those people but I can at least articulate them to you to add ... there may not be a silver bullet for this but at least if informs your debate, both in terms of the how the States is using surveillance, but also the concerns that individuals have about the way it is being used in the domestic sphere.

**Deputy G.P. Southern:**

I think there is a conversation we are still to have about individuals' private use of C.C.T.V. But before we do that can I just go on to some questions about the level of surveillance. In particular I am thinking about employees, and the general question would be, is it reasonable that in an 8 hour shift, there is a camera on you all time? Now, what is reasonable in terms of employee relations in terms of surveillance?

**Data Protection Commissioner:**

You must not confuse the regulatory controls of data as to questions, almost ethical questions, of the scope of surveillance. It is quite clinical in terms of data protection. It is not to say that those questions are not legitimate, it is just that they may not sit with me. Employees often get frustrated because I cannot ... I can take a view on the location of the cameras, in the same way that if the phones are monitored all the time that we say to employers that should have a phone where they can make a call to their G.P. (general practitioner) about the issue that their child has or they have that is private. There should be a private space for employees, but when they are performing their contractual duties I can say no more to the employer than you have to abide by the rules. Does that make sense?

**Deputy G.P. Southern:**

Yes, and the rules include ...?

**Data Protection Commissioner:**

Transparency, accountability, access, security, all that stuff we talked about.

**Deputy G.P. Southern:**

What is the purpose and what is reasonable to fulfil that purpose?

**Data Protection Commissioner:**

Yes. I had someone only last week who had ... was having a camera installed literally above his workstation. Really, really unhappy, and you understand why. When you have a camera in your face it makes you feel different, there is something about it, you know, the social science professors you have on the panel are better articulating that than me but it is about human autonomy, it is about a whole host of complicated issues that are the nature of being human, but I cannot really help because what I am saying, what our job is to say: “This is the rule that applies when you placing data, these are the rules that apply.” You have to apply those. But in a sense the moral and ethical questions about how far you go ... I can say you cannot put it in the staff toilets but I cannot say you cannot cameras full stop.

**Deputy M. Tadier:**

So who should be saying that, if anyone at all?

**Data Protection Commissioner:**

Good question. If you have got a union, possibly the unions, I don’t know, but the employer will argue that they are monitoring contractual obligations.

**Deputy M. Tadier:**

What about clearer legislation? Is that perhaps needed?

**Data Protection Commissioner:**

The trouble is you get into the realm ... in some organisations they are monitoring phone loans of dealers in banks, they rely on that very heavily. So the difficulty the Data Protection Law has is that if you make very rigid rules, because it applies to every bit of data, what might work there suddenly looks ludicrous with your privacy information for Boots Advantage card as opposed to mechanics.

**Deputy M. Tadier:**

To take a central example, which is cameras in toilets or changing rooms, that seems to be universally accepted that that should not be the case because that is just disproportionate. If that were a legal requirement, if it was just in the laws that says you are not allowed to install cameras in public changing rooms, you would not have to get all those inquiries. What would happen if somebody came to you and said: "We want to put a camera in the staff toilets?" Would you give words of advice?

**Data Protection Commissioner:**

Yes, I have never, ever had someone who has not listened to us but, you are right, in principle they could say: "Well, thanks very much for that but I am still going to do it." But I feel quite strongly about that so I think I probably would take it the whole way. We would issue a notice and if they appealed it it would go to a court. That is, in a sense, where you need to have these discussions, it is not just about what I think, it is about what the system thinks and then you work on precedent, because it should be me more than just one person's view. You base it on your years of experience and advice but ultimately ... I would very strongly about that, especially if it is young people, they should not be videoing them when they are changing or going to the toilet. So I probably would take that all the way.

**Deputy M. Tadier:**

A nightclub, for example, might argue that the toilets are where the majority illicit activity would happen, drug taking, et cetera.

**Data Protection Commissioner:**

Not that I know of, but again, and I hate to say this, I do not know whether there are cameras in there but we would be surprised.

**Deputy G.P. Southern:**

Can I take you on to another case where we were told by the Education Department that there is little, if any, use of C.C.T.V.s in schools, and yet we know one school where there is a non-monitored C.C.T.V. system which covers corridors and some classrooms for the protection of the children. Again, this is about level, is that appropriate? I can the function of that, it is to protect children and therefore it is reasonable. But C.C.T.V. cameras in school, permanently on, is that appropriate?

**Data Protection Commissioner:**

The law does not differentiate between age groups or vulnerabilities, interestingly. But I think there are moral and ethical questions which inevitably get raised when you are talking about young people. I am surprised by that answer, I will have to go back and check but I think a lot of schools are notified for C.C.T.V. usage.

**Deputy M. Tadier:**

What we found interesting and we have to look into this more, is that again with the purpose of filming, is that one school appeared to tell us that it is for supervisory purposes but yet they are telling us nobody is monitoring the cameras, so it seems they cannot be for supervisory, it could be for other security purposes, it is difficult to know.

**Data Protection Commissioner:**

It is probably something your professors would be better able to speak on than me but there is a deterrent factor, is there not? It seems to be people who install it will talk about it. I do not have any knowledge of that but I am just aware that is an argument they use, that is why dummies are sold.

**Deputy M. Tadier:**

But when schools do apply, they would have to register with you, would they, individually?

**Data Protection Commissioner:**

Yes, they are all separate data controllers, yes.

**The Connétable of St. Martin:**

Can we move on? Unless you have anything more?

**Deputy M. Tadier:**

No, I think we can move on to the last part.

**The Connétable of St. Martin:**

Yes, we have covered the States control of C.C.T.V., we have covered shops and that and then we get the private homeowners, who we spoke very briefly at the beginning I think, there is no control at all. If I want to put a camera on my house today at home, I could put a camera. I would not have to come and see you.

**Data Protection Commissioner:**

It would benefit from what is called the domestic use exemption.

[11:15]

**The Connétable of St. Martin:**

Domestic use is defined, I take it?

**Data Protection Commissioner:**

For personal or family use.

**The Connétable of St. Martin:**

Personal or family.

**Deputy M. Tadier:**

Is that for data or is it for ...?

**Data Protection Commissioner:**

Data.

**Deputy M. Tadier:**

Not specifically to do with cameras?

**Data Protection Commissioner:**

No.

**Deputy M. Tadier:**

Okay. Because you talked about the shops before, there is an exemption for small businesses but they are not exempt from cameras?

**Data Protection Commissioner:**

It depends on what they are processing but the C.C.T.V. would not fall within those definitions.

**Deputy M. Tadier:**

But it does for private individuals?

**Data Protection Commissioner:**

There is a broad domestic use, basically what the law ... the law sets out rules for people except in their own homes, essentially.

**The Connétable of St. Martin:**

Now, that is a camera inside the house, if I have got it on the outside of my home and it crosses on to the road ...

**Data Protection Commissioner:**

It is still on your property for your own purposes.

**The Connétable of St. Martin:**

But it crosses the road, maybe?

**Data Protection Commissioner:**

We often get that and they say: "Well, my car is parked there and it has been vandalised."

**The Connétable of St. Martin:**

That will always be the excuse, will it not, my car was vandalised?

**Data Protection Commissioner:**

Yes, I am telling you the feedback we get and a couple of times, where there have been children involved, we have referred it to the police because it could constitute harassment. But the vast majority it is neighbours at war and there is either an issue about vandalism or dog mess, cat mess, that is a common one, wanting to know whose cat it is. Or very often it is just because they know it will rile a neighbour and it does. It invariably does.

**The Connétable of St. Martin:**

It could be recorded on some sort of equipment inside and kept.

**Data Protection Commissioner:**

So easy, yes.

**The Connétable of St. Martin:**

No controls over it. Do you think there is a need for it to change?

**Data Protection Commissioner:**

I think that is a huge question, because what you are saying essentially is that do you want the Data Protection Law to extend to the domestic sphere?

**The Connétable of St. Martin:**

We are looking at it at the moment for the safety of buildings and I know the Minister for Health is doing a consultation, going into properties to see if they are safe. I guess it would be another one, would it not, because you are ... Sorry, go on.

**Deputy M. Tadier:**

No, no, I should not interrupt you, carry on,

**The Connétable of St. Martin:**

No, it is all right. We would be doing the same thing, imposing conditions on somebody on what they want to do in their own home or in their own garden.

**Data Protection Commissioner:**

That is a very complex question but I think in terms of domestic use the ... I think what was envisaged is that the processing would not have an impact. So if I had my Christmas card list on my laptop at home, they are my friends, my family and there is no adverse impact in terms of privacy. The challenge now, with this, is that if put a camera up and it covers your back garden, quite overtly recording images from your back garden which you like to go into with your family and your friends, that has a very, very real impact on the people being watched.

**The Connétable of St. Martin:**

Without a doubt.

**Data Protection Commissioner:**

So the domestic processing in this context is impacting other people in the way that domestic processing of a Christmas card list on my laptop is not. So the reach is wider, so this is where dialogue is important, because what do you want, if anything, to reduce the impact on those third parties?

**Deputy M. Tadier:**

The question is then, would you like more powers to be able to deal with domestic issues relating to surveillance?

**Data Protection Commissioner:**

I am not sure it sits comfortably with what the Data Protection Law is designed to do in the first place. I think there are real challenges to that, and indeed a scrutiny panel over a year ago now heavily criticised our office for seeking what I viewed as quite a minimal intrusion into what could be argued the domestic sphere. So I am getting conflicting views politically about what is wanted and I think essentially politically somebody needs to take stock of what this will mean once you go into the domestic sphere and how that will impact everybody.

**Deputy M. Tadier:**

To drill down, I guess the question is, is data different if it is collected by the state than if it is collected by a private individual?

**Data Protection Commissioner:**

The data itself is not different but the rules that sit around it are very different.

**Deputy M. Tadier:**

Just to following on, should that be the case? If the data is the same then your department should be interested in the pure data.

**Data Protection Commissioner:**

But do you want me interfering with people's Christmas card lists on their laptops at home?

**Deputy M. Tadier:**

No. If we keep it relating to surveillance. I just think there is a difference between which way the camera is pointed. For example, there is a police camera on Burrard Street which is, I think, attached to somebody's house. They must have permission to put it there. But any private individual could have exactly the same camera in a comparable location which would have the same scope. So the data they have is exactly the same but they are not even bound to tell you about that.

**Data Protection Commissioner:**

We spoke before about the implications of the processing. Now, if it is Joe Bloggs, it probably just riles the neighbours, if it is police the potential harm is significant for an individual, in my view.

**Deputy M. Tadier:**

But there is a counterargument, I guess, that the police have got the processes in place so they are bound by best practice you would hope and they have got all these other processes where the individual is not, so you could have a rogue neighbour who uses that for nefarious purposes.

**Data Protection Commissioner:**

Absolutely. I do not disagree with you and it is one of the reasons I am keen to be here and I am keen for you to have the discussion, because I think it extends beyond the legal framework that I am responsible for overseeing, but I think it is a very important question.

**Deputy G.P. Southern:**

As it borders on potential for harassment, the perfect conversation is with the Minister for Home Affairs.

**Deputy M. Tadier:**

That is the question.

**The Connétable of St. Martin:**

Or is it Planning?

**Data Protection Commissioner:**

I was just about to mention that because there was only one case I knew of where I think it was either because it was a certain type of field or a certain type of property, I cannot recall now, it was a couple of years ago, that they required planning permission for the camera. That was a much cleaner tool than anything else. As far as I am aware that was refused. So that may be an avenue because visually if everybody had them it would impact, and especially ones on poles. So there are a whole host of areas that are open for discussion but as a human being I feel empathy for the people that are affected. So just on that basis it is important that you know the sort of inquiries we are getting. Because, strictly speaking, I could say to them: "Sorry, I cannot help you, goodbye." But we try and give them good advice, good sound basis for advice, and sometimes that is harassment, sometimes it is a civil route. There are routes available to people but it is not easy.

**The Connétable of St. Martin:**

What Deputy Tadier was saying there before, and we think that in the proposed new police station, the police will have a camera on their building but it will have to be masked to prevent it going into private?

**Data Protection Commissioner:**

Yes.

**The Connétable of St. Martin:**

Next door, which is as close as you are to me, you have private that can have a camera which can overlook the police station?

**Data Protection Commissioner:**

Yes.

**The Connétable of St. Martin:**

It is just nonsense, I think. So nothing to stop it happening. Has there been a discussion between the Minister for Planning and your department at all in relation to this?

**Data Protection Commissioner:**

No.

**The Connétable of St. Martin:**

There has been nothing?

**Data Protection Commissioner:**

No. It would be a place naturally that we would go to, I just recall that there was one incident that involved Planning. Mostly it will not require planning permission, as far as I understand they would not normally.

**The Connétable of St. Martin:**

What proportion of people do you think come to your office complaining about private cameras compared to State owned cameras or shop cameras?

**Data Protection Commissioner:**

The vast majority is about private. That is why the stats would not be helpful to you.

**Deputy G.P. Southern:**

Sorry, the vast majority of inquiries?

**Data Protection Commissioner:**

Yes. That is why the stats would not be helpful to you, because the stats are about corporate processing and mostly people are reasonably happy with that. So just giving you stats on that, you would think: “Oh gosh, nothing really to worry about” but anecdotally I go back to that point, it is important that you get the feedback that we are getting increasing inquiries and you can pop along to any shop now and buy this equipment cheaply and easily.

**Deputy M. Tadier:**

I wanted to ask about the human rights aspect of it. Under Article 8, as you know, there is a right to respect the private and family life. I guess the first question is how does that impact on your department with respect to surveillance?

**Data Protection Commissioner:**

It does not, in a word, because while the Data Protection Law was born out of privacy concerns, data privacy concerns, so that is where its birth parents are, I am a creature of statute so I can have a moral position on surveillance, which I do, and I can have a position on privacy, which I do, but ultimately I have to abide by what the law tells me to abide by. Now, I have got many years of experience of working in areas of privacy so I can talk to you about these things, but what I cannot do is go back and enforce them. So I think there is a distinction here, and I think that is exactly as it should be. I should not be off on frolic because I feel ... I am elected and the law is there for a reason, so I work within the constraints of the law and it is up to the lawmakers and the politicians in any Government to establish where there is a gap or whether things need changing based on experience of people at the coalface. I think that is what this process is helpful for. But in terms of how does Article 8 impact me, the Data Protection Law is E.C.H.R. (European Convention on Human Rights) compliant, something may massively impact someone's privacy but there is nothing the Data Protection Law can do about it. It is not to say I do not care, but it is to say that technically speaking the law does not give me the tools.

**Deputy M. Tadier:**

One area of concern for us is how does that individual ... we have had at least one person come to us with that specific problem about a neighbour dispute with a camera that is looking over into his property, and that has affected him quite acutely. He will have a reasonable expectation for the right to privacy, which the state should in some way give him that assumption, but how does he enforce that. Who would he go to? Where is the lacuna, if there is a lacuna?

**Data Protection Commissioner:**

Sadly, exercising rights comes at a cost a lot of the time. It is not just true in this area. It is not just true in privacy, it is true in a lot of areas. The state will intervene in certain circumstances but essentially if it is not harassment you have to get yourself a lawyer.

**Deputy G.P. Southern:**

Human rights enforcement is based on a specific case being brought. So while we still have not had a case under human rights in Jersey, despite having the law, while no cases are brought it still remains wholly enforceable.

**Deputy M. Tadier:**

But is one of the solutions - we are going to have to try and make some recommendations to resolve that area - that we give data protection more powers to oblige domestic camera users to register with yourselves if they are monitoring something other than their own property?

**Data Protection Commissioner:**

Possibly, it is worthy of discussion.

**Deputy M. Tadier:**

Would that be an issue for you?

**Data Protection Commissioner:**

Administratively, no, because we already run an administration system which requires organisations to do so. I think you would have to think carefully about what it would cost, the practicalities of it. You do not really want to be charging people, I would suggest it would not go down that well. You have to be clear about what you expect from me in terms of interfering with the domestic sphere of individual's lives and what happens if they do not? Again, it is easy to criticise our office for taking certain action under the law, we would be open to even more of that criticism, so we need political support for anything that is given to us, and that is really quite important. But I think it is an area that deserves some serious consideration.

**The Connétable of St. Martin:**

Shall we move on? Just a couple of small points, I know time is going, sorry. The body cameras that were featured in last night's *J.E.P*, I do not know if you have any views on this, I take it there is no legislation to cover that part of it or would there have been ...

**Data Protection Commissioner:**

Yes, it is all covered.

**The Connétable of St. Martin:**

You do exactly the same?

**Data Protection Commissioner:**

Yes. Yes, all covered, which is a good thing. We spend a lot of time and energy on ensuring that the most important areas of data processing in Government, which are policing, health, education, where young people are involved, social services, they have very well supported data protection officers in place that are experienced to understand the issues and we can have an honest and open dialogue where that is terribly important. So early on in any process where there is new data

being collected there is a dialogue with our office and we give our view about certain things. They need a very good policy on that, on the handling of that. We have seen that policy. It is good quality policy.

**The Connétable of St. Martin:**
The States Police policy?

**Data Protection Commissioner:**
Yes. It talks about portality, it talks about fairness, it talks about security, all those things which they should already be well-versed in. Because this is just a slightly different technology but it is the same principle as any surveillance they undertake. It is triggered, it is not constant, and there will be a warning given, for example, if the cameras are being turned on.

**The Connétable of St. Martin:**
By the officer?

**Data Protection Commissioner:**
Yes. So bearing in mind I cannot take a moral view of the surveillance, this is a legal view that they are, as they have set it out at the present time, doing so within the confines of the Data Protection Law.

**The Connétable of St. Martin:**
Will audio be the same?

**Data Protection Commissioner:**
Yes.

**The Connétable of St. Martin:**
So St. Helier parish wardens who have an audio, they have to advise somebody if they are going to activate it. You would not be able to tell if it is complied with, that the police officers are complying with ... they should comply with codes but you are not policing them.

[11:30]

**Data Protection Commissioner:**
One of the things about individuals interacting with the public sector is that they tend to be reasonably confident at complaining, being able to complain, which is a good thing essentially. So I think that most complaints relate to public sector because, as I say, the interaction from the

system is not voluntary so a vast amount of processing goes on. We are very alive to these questions and we take a very keen interest in how they are managed at police level. So every so often I will ask to the C.C.T.V. control room, for example, and pick a random camera and see if it is blocked, the camera was blocked last time I went, because it should not be able to get into next door's window, if it is still blocked or they just do it when I turn up. It is not a lot but we do some things and we obviously have to react to any complaints that arise. Because they are incident driven these cameras, if a legal representative were to be involved in a case for his or her client that involved the collection and use of those images or audio, and they were concerned, the first they come is to us. So I think there is enough of a checking mechanism, I would hope, to make sure they do this properly.

**The Connétable of St. Martin:**
If a private citizen is using a camera or something like that, there is no controls at all?

**Data Protection Commissioner:**
No, domestic use.

**The Connétable of St. Martin:**
Domestic again? I can recall an incident 2 or 3 years ago where a member of staff in a public building observed something from the back window, a chap attempting to break into various rooms of someone's house and filmed ... took pictures and when the States Police arrived they were more concerned this person had taken photographs and recorded and should not have done it, rather than the person who had ...

**Data Protection Commissioner:**
I think you will see that shifting a little bit because they use ... most police forces now recognise that everyone is a photographer out there because your phones now are all ...

**The Connétable of St. Martin:**
The Berrick(?) murder recently in the U.K. Everybody filmed it.

**Data Protection Commissioner:**
Exactly, so I think law enforcement recognise that it can provide a useful tool for evidence. That domestic use. But I think it is difficult when you are shifting from one manner of processing to another. Culturally things are changing in terms of how we use data, how all of us have equipment that can record ... you can buy these little planes with the cameras on. Have you seen the reports of that? They are domestic and they can go anywhere. Really extraordinary capacity to record.

You can buy them online, they are remote controlled and they can go anywhere, right over your garden, it is an interesting challenge ahead, I think.

**The Connétable of St. Martin:**

The public can film the police, no problem, at an incident but the police cannot film the public without ...

**Deputy M. Tadier:**

Have you tried filming the police before?

**Data Protection Commissioner:**

Depending on the context I am not sure they would welcome that terribly. I think it easily becomes adversarial when things like that are done without mutual consent. The rules that apply to government necessarily have to be higher than the rules that apply to the vast majority of the public. I think that is pretty clear. It is where those rules finally rest that is an important question.

**The Connétable of St. Martin:**

You would not know but are you assuming that the body cameras are going to be extended throughout the force in time, depending on this ... that is not really a question for you, I suppose, but you would not have objections?

**Data Protection Commissioner:**

I am always careful with my language here because, you know, someone said to me yesterday: "Do you support the use of these cameras?" No, I do not support but I will say ... it is not that I do not support them, I cannot take a moral view, all I am saying is that they either do it in compliance with the law or they are not. From what I have seen there is a framework around how they are to handle this data and they are complying with that framework. That is as far as I will go.

**Deputy M. Tadier:**

There is presumably a spirit of the Data Protection Law which underlies everything that your department does. Is there any way you could summarise that? That is maybe a big ask.

**Data Protection Commissioner:**

No, it is about giving people some control about what happens to their own data. It is about ensuring when people are not able to exercise that control: "Will I give my information to the tax man?" You know, most of us do not want to give information to the tax man, we have no choice, or the police force, we do not have a choice. So where we do not have a choice about that there

is a fairness around how that information is handled. I think that, in really general terms, is how I would sum it up.

**The Connétable of St. Martin:**

Can I just ask a question about filming in cells, prison cells? Do you think it is right that someone should be filmed 24 hours in a cell, have a camera on them all the time?

**Data Protection Commissioner:**

Again, if you can sit across from the person that is making a decision about that and ask them why and get to a decent answer, not just because we can but because ... you know, I cannot speak for the police. But your answer may be: "We have had 15 incidents where police officers are injured." "We have had 15 incidents where prisoners have been injured." "We have had cases where lawyers have been cross we have not been able to prove or disprove something." So you would want a good answer back to the very, very simple question of why. You put that to the decision makers and you want an articulate clear response. If you do not have an articulate, clear response they should not be doing it.

**The Connétable of St. Martin:**

So if there is a camera in a cell you are relying that it is not switched on unless you want it on. Someone comes into this room and there is a camera there, we do not know ... the tapes are on today but they will not be on in an hour's time when we do something else. So a prisoner sees a ... should they be in a different cell, should they ...

**Data Protection Commissioner:**

That is a good question. The body camera, I think, will have a light. I have seen one. But I think there will be something indicating that it is recording. That is all part of the spirit of openness. So whether that is something that could be explored with the force, I do not know.

**Deputy G.P. Southern:**

In some circumstances it is for the protection of the individual in that cell. That happens regularly down at the P.R.C.(?), for example, it is monitored by camera and an hourly visit to check breathing.

**Deputy M. Tadier:**

Following on from that, it is clear that in some cases if there is someone on suicide watch, they may want to employ a camera rather sit in there. But if somebody had a camera that was not recording, it was just streaming live so they could supervise, would they need to notify your department?

**Data Protection Commissioner:**

Yes, we have taken the view that live streaming constitutes processing. It is an interesting question. I always look at the potential impact and if you are just live streaming from a kid's changing room, should that mean that you are not covered? I do not think so. So we have taken the view, although it is challengeable, that does constitute processing and therefore does need to need to be notified.

**Deputy M. Tadier:**

But where is the data?

**Data Protection Commissioner:**

In transit.

**Deputy M. Tadier:**

I guess the data is being transmitted to our brains, is it not? It is just the medium.

**Data Protection Commissioner:**

Yes, it is the potential. If I am looking at you I cannot somehow show lots of other people. If you are in a changing room with somebody else, the fact there is one other person in there with you is not going to be a detriment to your privacy ... well it might be, but not in the way if I was sitting with a iPhone and it was streaming across on to an internet site.

**Deputy M. Tadier:**

Yes, and it could be recording ...

**Data Protection Commissioner:**

I am sure if it is live stream they have a capacity for capture as well.

**Deputy M. Tadier:**

I think that is all that I have.

**The Connétable of St. Martin:**

Can I thank you very much for all you have given us today? I do not know if you have the time now, if there is any other comment you want to make to us to give you the opportunity that might help in our final report and submission?

**Data Protection Commissioner:**

I think I have probably covered everything and I have not rattled on for too long, but I think it very helpful this discussion is taking place and I have been very glad to be part of it. I think these are important questions, but I think there needs to be a lot of consideration before extending the reach of the law into the domestic sphere from a data protection perspective.

**The Connétable of St. Martin:** Thank you very much.