



Children, Education and Home Affairs Scrutiny

Panel

What protection do children in Jersey have from
online harms?

Witness: Information Commissioner

Monday, 7th July 2025

Panel:

Deputy C.D. Curtis of St. Helier Central (Chair)

Connétable M. Labey of Grouville (Vice-Chair)

Deputy H.M. Miles of St. Brelade

Witnesses:

Mr. P. Vane, Information Commissioner

Advocate D. Blackmore, External Local Counsel, Office of the Information Commissioner

[9:30]

Deputy C.D. Curtis of St. Helier Central (Chair):

Welcome to this special hearing about online harms with the Information Commissioner. Today is 7th July, and I would like to draw everyone's attention to the following. This hearing will be filmed and streamed live. The recording and transcript will be published afterwards on the States Assembly website. All electronic devices, including mobile phones, should be switched to silent. I would ask that any members of the public who have joined us in the room today do not interfere in the proceedings and, as soon as the hearing is closed, please leave quietly. To begin with introductions, I am Deputy Catherine Curtis, the chair of the panel.

Connétable M. Labey of Grouville (Vice-Chair):

My name is Mark Labey, Connétable of Grouville, and I am the vice-chair.

Deputy H.M. Miles of St. Brelade

I am Deputy Helen Miles of St Brelade, and I am a panel member.

Information Commissioner:

I am Paul Vane, Information Commissioner for Jersey.

External Local Counsel:

I am Advocate Davida Blackmore. I am External Local Counsel to the Office of the Information Commissioner.

Deputy C.D. Curtis:

Thank you everybody. I just want to say thank you also for the written submission to the panel and for coming in to speak to us today. We have one hour for this hearing. First of all, I have got some questions - quite long questions - but they are about the role and the mandate, and the effectiveness of any changes as well, and so on. Commissioner, in your written submission to the panel, you have outlined the powers of the Jersey Data Protection Authority and highlighted that the powers are targeted at addressing data protection related harms such as tracking, lack of transparency and unlawful processing by online platforms rather than broader harms, like dealing with harmful or illegal content or cyberbullying. Could you summarise how effective you think these powers are in dealing with issues and harms that are impacting children in online spaces?

Information Commissioner:

Sure. I think, first of all, it is important to say that the Data Protection (Jersey) Law is technology neutral. It sets a framework of principles which are designed to afford protection to all individuals of all ages in respect to their personal data. Many of those principles are helpful in terms of preventing online harms. For example, data retention limitations, which can, if they are strictly adhered to, prevent organisations from holding data for longer than it is necessary. But our powers are limited to enforcement against data controllers. That is organisations, in the main, who collect personal data from individuals and determine the manner and the purposes for which that information will be used. Our existing powers at the moment do not currently extend to enforcing against individuals who, for example, post harmful content on social media platforms in relation to other individuals. Those cases currently sit within the remit of the police if they fall into the criminal sphere, or if it amounts to harassment, or it may fall within the scope of the terms of use operated by the respective social media platforms. I think just to summarise that, the Data Protection Law is not designed for person-to-person matters generally, but rather for business-to-person issues where the rights of the

individuals under the Data Protection Law are not being upheld. It is about balancing the demands and the powers of the businesses compared to the individual.

Deputy C.D. Curtis:

Okay, so where it does not cover individuals, if it is illegal, then the police can deal with that?

Information Commissioner:

Yes.

Deputy C.D. Curtis:

But if it is not illegal, like it is more general harms and cyberbullying, then there is not anything currently, or not completely to cover that.

Information Commissioner:

No, not unless it falls into the regulatory remit that we have.

Deputy C.D. Curtis:

Okay, thank you. Commissioner, your written submission notes that while the J.D.P.A.'s (Jersey Data Protection Authority) powers under the Data Protection Authority Law are increasingly relevant to online harm, where such harms involve the misuse or mishandling of personal data, it is very important to acknowledge that Jersey's data protection framework was not designed to operate as a comprehensive online safety regime. Given this, do you see the J.O.I.C. (Jersey Office of the Information Commissioner) acting, at least in practice, as the Island's de facto regulator for online cards?

Information Commissioner:

No, not really; not at this moment in time. I think, because the law sets out quite a strict regulatory remit for our office, which is very much based on the European General Data Protection Regulation ... we can provide advice, we can provide signposting, we receive inquiries or complaints around online harms, and of course we will deal with any regulatory issues that fall within the scope of the law. But in general terms, our remit does not currently extend to dealing with enforcing or dealing with those kind of incidents. Those other authorities, such as the police, are better to handle those matters through their criminal investigatory powers. We have an M.O.U. (memorandum of understanding) with the States of Jersey Police, which ensures that we can share relevant information with them when the time arises.

Deputy C.D. Curtis:

My next question actually leads on from that because the Government's forthcoming law and other work may expand expectations of J.O.I.C. From your perspective, what additional responsibilities are likely to fall to you?

Information Commissioner:

I think that is largely a matter for the policy makers in Government to decide. But if you are asking for my professional view on what is clearly an important topic such as this, I would very strongly advocate for separate legislation that is clear and is proportionate and the right fit for Jersey with full collaboration with all relevant stakeholders; for example, Children's Service, Education Department, Children's Commissioner, States of Jersey Police, government policy makers, law draftsmen and our office as well. I would also say I think it should involve young people themselves, who I would argue are very much quite often far better placed to see the potential harms and identify what solutions would be the most practical and effective for them. But wherever the suggested resting place or oversight of any online harms legislation should sit, I do agree that it may fit better with our office rather than create a new regulatory authority, for example. But it will be critical to its success to ensure that the oversight body is appropriately resourced, both in terms of financial and human capacity and capability. Any solution needs to be future-facing, practical and enforceable. I think that is a key point, and have the ability to keep pace with technology. It should also be consistent with other global legislative frameworks that allow for interoperability and efficiency of enforcement.

Deputy C.D. Curtis:

Thank you. The next question also develops this, that the Minister for Children and Families has recently confirmed in the States Assembly that the Government is giving consideration to a strategy to address online harms to children. Can you advise us what would you expect to see included as part of that strategy from a data protection perspective?

Information Commissioner:

You will have to bear with me as I have quite a long answer to this one. I think any strategy must be able to deliver on what it sets out to achieve in the first instance. There is absolutely no point in creating legislation that is either ineffective or fails to protect people that it was designed to protect or is not practically capable of being enforced. We have seen the scattergun approach too many times in history to know that we cannot just legislate for whatever we perceive the harm to be, shouting loudest at the time might be. So we would recommend a long-term holistic view with a focus on future threats and future protections, with the ability to adapt as needed as the environment changes. I think it is also important to say that we must recognise that online harms is not just about social media platforms and mobile devices or algorithms. It goes much deeper than that. It is about a myriad of information, misinformation, disinformation that young people are exposed to and including, but not limited to, sexual content, radicalisation, gang cultures, self-harm, suicide. You

have seen other people talk about this. I think we should try and avoid, wherever possible, a reactive proposal that does not address the underlying problem, or worse, fail to provide the appropriate protections for those that we are trying to protect. I saw from the Public Health submission, they suggested a societal approach being required. I would tend to agree with that submission. But while it is important that young people and teachers and parents, all of us, we have a shared responsibility for this, it is equally important for the technology companies and platform providers themselves to be held to account and take significant responsibility for their actions. There has been some significant improvement in recent years, but there is still a lot more work to do. I think a whole Island multidisciplinary approach is required because the regulator cannot do it on their own. It is that simple. We must at all costs avoid the unintended consequences of rushing through any legislative framework without full and careful consideration with all relevant parties involved because, again, technology moves too fast. We do not want to waste time getting it wrong. In terms of a data protection online harm strategy, that should focus on privacy first, and more specifically privacy by design; age verification technologies, education, and a robust enforcement capability with accessible remedies for those affected. The whole concept of what constitutes harm and what type of activity that word is actually meant to cover will be essential to nail down, as well as understanding that most of the problems with the internet are down to a common thread of corporate surveillance, monitoring our behaviours and our preferences continuously. There are many strategies that we could consider. Some commentators on the subject have suggested, among other ideas, banning online behavioural advertising to remove the opportunity to weaponise children's preferences and limit their ability to track children. But I think what is really needed is a will to think beyond our natural emotional responses and devise carefully considered practical solutions by design. Another feature of a strategy such as this could benefit from is addressing that power imbalance between the user and the platform provider, making it easy for actions to be brought, putting much of the control back in the hands of the user. So looking at simple things like opt-ins rather than opt-outs would be a solution. You could also draw inspiration from the Digital Services Act and also worth looking at other programmes and codes of practice, such as the ProCoM (Project Online Content Moderation) in the Netherlands, which facilitates the application of the E.U. (European Union) Digital Services Act to combat illegal content. That is a public-private partnership where citizens, government, and the internet sector, they collaborate and can act more efficiently where online harms and illegal content is identified. It allows for easy reporting of incidents as well as providing advice and guidance and building that knowledge capacity among providers.

Deputy C.D. Curtis:

That is really interesting, thank you. I will just quickly ask you, when you mentioned how important it is to try and nail down what online harms actually are, do you think there ... because this is such a huge thing and it keeps changing and developing, do you think there is a danger in things not being addressed that are currently a problem?

Information Commissioner:

Absolutely, which is why it needs to be flexible and adaptable to address future harms and be able to deal with those because if it is too restrictive, as some commentators have said about the U.K. (United Kingdom) Online Harms Act, that it does not ... it is too backward thinking. It does not look forward enough and consider actually changing technology realises changing harms. You have to be able to try and predict the future a little bit.

The Connétable of Grouville:

We have heard that criticism as well, Chair, have we not?

Deputy C.D. Curtis:

All right, thank you.

Deputy H.M. Miles:

You talked a little bit there about future legal protections and what that might look like. If we just talk about current legal protections, what provisions have we got in our Data Protection Law that offer the greatest day-to-day protection for children?

Information Commissioner:

I think there are a few specific provisions in the law at the moment that relate to children because the rights afforded to individuals under the law are for all individuals, not just children. But there are a few that can be particularly helpful when safeguarding children from online harms. Firstly, the lawfulness, fairness, and transparency principle. That is a core principle that ensures that children's personal data is processed lawfully, fairly, and in a way that they can understand. The benefit for children with that is that organisations are supposed to clearly explain, in age-appropriate language, how children's data is used, and it helps prevent misuse or hidden data practices, especially online, for example, in apps or games collecting, where clear consent is not there. You have the right to erasure, not the right to be forgotten, as it is often called. Children or their parents or guardians can request deletion of personal data when it is no longer needed or when it is collected unlawfully. Of course, that benefits children because it allows children to remove data they have shared online, perhaps impulsively or unknowingly, perhaps somebody else has posted something. It helps limit long-term digital footprints, which is crucial for future privacy. Then you have parental consent for information society services. I will talk a bit about that in a moment. That is where consent is required for the processing of children's data in online services, so that is things like gaming and social media, where the child is under 13. That has got to be given by somebody with parental responsibility. That protects young people from signing up to services like social media or gaming platforms that might exploit or mishandle their data and ensures parents are involved in decisions

about their future. So I guess those provisions, along with the general rights afforded individuals under the law, they work together to safeguard children's privacy, ensure appropriate adult oversight, and give them and their guardians more control over their personal data. At least that is the intention of the legislation. The law also allows us to approve codes of conduct, which include provision relating to information provided to and for the protection of children, and the manner in which that consent of the persons with parental responsibility is obtained.

[9:45]

Deputy H.M. Miles:

In your submission, you talked a lot about the outreach that you are doing in schools, et cetera. Based on the outreach and feedback, how well do you think children and parents tend to understand those protections?

Information Commissioner:

I think we have seen some drastic improvement in the last 3 to 4 years that our outreach programme has focused on young people, and certainly in respect of their rights to privacy under the Data Protection (Jersey) Law, which feed into that concept of online safety. So our Young Privacy Ambassador Programme, we expanded that just post-COVID in 2021, and we have delivered 44 sessions to Island schools via a mix of in-person and virtual delivery of key messages. That programme is designed to educate young people about why their personal information should be protected and aims to equip them with the tools that they need to do so. We have followed students, their progress through their school journey with workshops such as our courtroom challenge, which Advocate Blackmore is heavily involved with. That offers a deeper understanding, deeper level of education around privacy rights and ethics. Following the sessions that we did in 2021, 80 per cent of the young people that we engage with commented that they understood the importance of protecting their personal information. The following year in 2022, as part of that same programme, we reached out to over 500 secondary schools students, encouraging them to challenge their considerations of privacy through similar workshops in classroom learning, school assemblies, talking about things like what is personal information and how can it be protected, to information about their rights under the law and basic data protection principles. In 2023, we saw a further expansion of that engagement. We added a community youth worker to our team and that allowed us to hold more in-depth workshops, privacy debates. We worked with the Education Department to develop an approach for key stage 2 staff to support the rollout of age-appropriate personal information safety sessions for children and young people. In total, we delivered those sessions to more than 2,500 young people in primary and secondary schools, youth clubs and scout groups in Jersey. Last year, we engaged with 26 per cent of the total population of under-18s across 18 different schools; 86 per cent of them said their knowledge of our office and protection of their

personal information and their understanding of their rights under the law have been improved as a result of those sessions. Lastly, we did 88 sessions to young people between the ages of 7 and 18. In addition to that, I think during workshops that we have done with the Children's Commissioner and the Youth Advisory Group, which comprises of young people between the ages of 7 and 17, we observed a much clearer understanding of how to get potentially harmful content taken down from platforms. For example, when they spoke about being exposed to pornography online, they reported that they just ignore it. They also said that they know how to report unlawful and harmful content. I think it became apparent to us during those sessions that perhaps we need to look more through the lens of young people as to what is acceptable or not to them rather than looking at issues through our own perceptions and perspectives of what we think is right or wrong for young people. In terms of the parents, that is a lot more difficult to measure. However, many parents are captured through our Parent Teacher Association and general community and business outreach sessions and public awareness campaigns. Overall, we have definitely seen an increase in general public awareness since 2018. What is really nice to see is that the parents are actually learning from their children following our school sessions. One parent commented that their daughter had told her about a visit from the J.O.I.C. to their year and said that it was the best P.S.H.E. (Personal, Social and Health Education) lesson that they had had that year, which I am thrilled about. Another parent said that their child took something away from our session without it being too overwhelming for them. So it seems that the message is getting through to parents as well as their children.

Deputy H.M. Miles:

Thank you. In the law, there is a domestic purposes exemption. We were just wondering if that leaves any gaps when harmful images are shared kind of peer-to-peer.

Information Commissioner:

Yes, you are referring to the application of the law, which is under Article 4, and that says that: "This Law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity (but applies to controllers or processors that provide the means for processing personal data for such an activity)." It goes on to say: "This law applies to the processing of personal data in the context of a controller or processor established in Jersey." I will not go into the details of the rest because I do not want to bore you with the complexities of legal definitions of data controllers or processors. But in the vast majority of circumstances, an individual will not be considered a data controller or a data processor for the purposes of the law. It certainly does not extend to the processing of personal data in a purely household context, when dealing with just a household activity, which in the main would include personal web browsing and posting on social media. Because of that, our powers and our remit do not extend to cover peer-to-peer image sharing.

Deputy H.M. Miles:

Okay, so playground stuff that we have heard.

Information Commissioner:

Yes. It ties back to what I said earlier, that our Data Protection Law governs how organisations deal with personal data, it does not cover information used by individuals.

Deputy H.M. Miles:

Have you had any conversations at all about the limitations of that domestic purposes exemption with Government?

Information Commissioner:

Not specifically that, but in general discussions around online harms and proposed new legislative reform. We have had a number of detailed discussions about the limitations with the Digital Economy team at Government explaining how the law is applied and its limitations in respect of taking enforcement action in particular against individuals who are not data controllers and therefore fall outside the scope of the law as it stands, and also how that mirrors the framework set by the General Data Protection Regulation in Europe. I think to expand data protection legislation to cover processing of information by individuals in a private capacity would be novel territory, and I am not sure ... I am certainly not aware of any piece of data protection legislation that strays into that area elsewhere.

Deputy H.M. Miles:

I guess we have other protections if that sharing is criminal through the Article 52 of the Telecoms, so where enforcement will be taken through police. So it sounds to me what you are saying is there is a very clear distinction between the data sharing, and actually the enforcement from a criminal perspective.

Information Commissioner:

Yes.

Deputy H.M. Miles:

Okay, thank you. You talked a little bit earlier about this age 13 consent threshold, particularly around the gaming. Have you got any evidence of how well that works in practice?

Information Commissioner:

I think it is important first of all to quash the myth that the reference to age 13 applies across the whole of the Data Protection Law. It does not. It is only in relation to information society services

or essentially non-face-to-face provision of online services usually for reward; financial reward that is. I think it is also important to define what “consent” actually means. The Data Protection Law says: “‘consent’, in relation to the processing of a data subject’s personal data, means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, whether orally or in writing, signifies agreement to the processing of that data.” Again I will not go into the full consent definition because it is quite long. But essentially: “A child under the age of 13 may not give valid consent to the processing of his or her personal data by a controller for the purposes of an information society service but valid consent on behalf of that child may be given by a person with parental responsibility for him or her.” The reality is it is almost impossible to identify whether or not this provision is working in practice, and we have certainly not received any local complaints or concerns to suggest otherwise. Most information society services who are responsible for ensuring that they have the appropriate consent mechanisms in place are either (a) not local, (b) exist in the shadows, or (c) have some provision through their websites and platforms that “require” parental consent where the user is under 13. But in practice, however, I suspect there are numerous users under 13 who have managed to circumvent that provision very, very easily. I mean, how do parents consent? How is it verified? Can you be absolutely sure that, given that the contact is faceless, that the user is over or under 13 and that consent is actually valid? My gut tells me that you simply cannot. I know from observations and comments that I have had from some of our colleagues are that some parents are signing up underage children to platforms, some underage children are circumventing parental controls to sign up to online platforms, some children use friends’ devices that do not have parental controls set up on them. I think the question is how far is the state prepared to go in regulating essentially the private lives of individuals or interfering with that parental responsibility. A law can do so much, but will it actually address or resolve the reality of the situation of the issues that we are trying to remedy here?

The Connétable of Grouville:

And indeed is it enforceable? Yes, thank you, Commissioner. I am going to be dealing with topics relating to enforcement and takedowns, if I may. Referring to your published data about enforcement activity, can you confirm if any of the complaints and/or formal inquiries related to children’s data?

Information Commissioner:

Not specifically in relation to any online platforms, however, we have issued public statements to C.Y.P.E.S. (Children, Young People, Education and Skill) and Children’s Services in the past, and they are all publicly available. We did have a case a number of years ago on which we issued a public statement where the Planning Department had uploaded information about a child’s illness on to the online planning application register. Of course, that was removed following our intervention, but other than that, no, we have not had anything.

The Connétable of Grouville:

Thank you very much indeed. Can you advise the panel when a person does approach J.O.I.C. in relation to an issue impacting a child or young person, what is the quickest, realistic timeframe for getting harmful material removed or is there one?

Information Commissioner:

The simple answer is no, because the law, it falls outside of our remit at the moment and we have no powers in that respect. We rely on relationships that we have with those social media platforms and providers and the contacts that we have there through their data protection officer networks to try and get those removed, but there is no formal process.

The Connétable of Grouville:

That leads on to the next question, how frequently have you needed to use stronger measures like deletion orders et cetera, but you have already explained that.

Information Commissioner:

No, there is none there.

The Connétable of Grouville:

Thank you. If the content sits on a platform based outside of Jersey, can you advise the panel what practical routes exist for enforcing an order?

Information Commissioner:

The J.D.P.A. has a positive obligation to engage with data protection authorities on cross-border issues, including sharing information and providing mutual assistance to other supervisory authorities with a view to ensuring that Data Protection Law is applied and enforced. An effective enforcement against entities outside of Jersey often hinges on our co-operation with other data protection authorities. How we do this depends on the issue we are dealing with largely but, for example, if an entity is based in another E.U. jurisdiction we may refer complainants to that data protection authority in that particular area, and that is because while the Data Protection (Jersey) Law may purportedly have extra territorial reach, practical enforceability again may be more easily achieved through collaboration with regulators who are in the same jurisdiction as that entity.

The Connétable of Grouville:

Do you have any examples that you might be able to give the panel and to the public that that has actually happened?

Information Commissioner:

Yes, one in particular, quite recently. Within the last 12 to 18 months, we are one of 11 data protection authorities that signed a joint letter to all social media companies in relation to the illegal practice of data scraping. This was in the wake of a case called Clearview AI, which was an organisation which essentially scraped the internet for information about individuals. That was a case jointly run by the Canadian and U.K. data protection authorities and the response so far from the social media companies has been very positive in that they are ensuring that the processes do not allow for that kind of activity in the future. The Cambridge Analytica case was another one, probably more well known than the Clearview. We have also had certain cases that relate to entities situated in Ireland, for example, and again complainants have been referred to the Irish Data Protection Commissioner, who have assisted in those particular matters.

The Connétable of Grouville:

Excellent, thank you so much. Should new legislation give the J.O.I.C. further enforcement powers, how would those be in day-to-day terms?

Information Commissioner:

It very much depends on what they are. Whatever enforcement powers are added, as I said before, we must be certain that they are effective and properly resourced and can be practically enforced in other jurisdictions, particularly outside of Europe where it becomes far more complicated, as I mentioned earlier. If any fall in enforcement proceedings needed to be initiated, then that inevitably will have a financial impact, and an impact on time and resources, and those things will need to be seriously considered when considering whether a matter ought to be pursued.

[10:00]

The Connétable of Grouville:

We have made the points quite vocally about Jersey's size, Jersey's demographic, if you will. Looking at the size of Jersey versus global platforms, how realistic is it to achieve enforcement internationally?

Information Commissioner:

It is not impossible. Absolutely not. But, again, for the reasons I have already mentioned, it is challenging at the moment. It is expensive, extremely expensive, perhaps some would argue cost-prohibitive, and it is time consuming, and it currently offers very little, if any, recourse to the affected individuals. That is really the crux of it, is that the people you are trying to protect are not getting that protection because you are too busy fighting long-winded court battles, which are expensive and, yes, not always appropriate.

The Connétable of Grouville:

Thank you. The Minister for Sustainable Economic Development highlighted the importance of the relationship built by the J.O.I.C. with other regulators and major tech firms. How comfortable are you with that model?

Information Commissioner:

It is far from ideal. As people move around and those contacts will not always be there, or be the same people that you have got that relationship with, but it does serve as a useful temporary solution where there is no other practical way of achieving the outcome needed, and it may be the most appropriate and fastest route to achieve the intended outcome at the moment.

The Connétable of Grouville:

Thank you very much.

Deputy C.D. Curtis:

Can I just add to that? You mentioned about working with regulators in other jurisdictions, but you have also mentioned about when it is outside Europe that can be more difficult. Is that like one of the biggest difficulties in that?

Information Commissioner:

Not that it comes across to us particularly often, but when we have had to deal with either a non-European or not non-adequate jurisdiction, and the U.S. (United States) is probably the largest and most complex, and that is where a lot of the social media companies, for example, and tech companies would be based. It does help when they have offices in Dublin, because that is a European jurisdiction, the European G.D.P.R. (General Data Protection Regulation) applies so that is much better. But if it is a non-adequate jurisdiction, and particularly the U.S., it is more complex.

Deputy C.D. Curtis:

Okay. Thank you.

Deputy H.M. Miles:

At present, do you think your office has got the staff, expertise, and budget to manage a possible rise in the child online harm work?

Information Commissioner:

That is quite a difficult question to answer without really understanding what our planned remit here would be, and what any rise would be expected to look like. But in essence, and having some idea

of what would be involved, no, is the simple answer. Our existing resource would not be sufficient by any means. We currently have a team of only 17 people, of which 7 are case workers and their responsibilities are very broad. They cover the regulation of nearly 8,000 organisations in terms of data protection, and that is just the ones that are registered with us, and the entire public sector in terms of regulation of freedom of information law. Any addition in powers and responsibilities imposed on my office would very likely need a significant resource injection, not just in casework either, but in outreach as well is the likelihood, and expectation would be for us to increase our output in terms of guidance and education, which would be in addition to our current statutory duties.

Deputy H.M. Miles:

Can you give us any sense of the scale of that resource?

Information Commissioner:

Without knowing what the remit is, and exactly what powers we would have and what we were charged with regulating, that is an impossible question to answer. We do not know what the volume of issues, for example, would likely be that we will be receiving. It is not even really possible to even guess the practical impact of those reforms and what they might have on our office in terms of time and resource. But like I said all along, careful consideration and full collaboration needs to happen before any changes are adopted. It will be futile to enact a piece of legislation or powers that are simply ineffective, do not address the issues that we are trying to resolve, and certainly do not provide the recourse for the individuals.

Deputy H.M. Miles:

Are you confident that you have got a sufficiently strong relationship with Government to be able to feed in these views as part of the policymaking process?

Information Commissioner:

Yes, I am. We have a good relationship.

Deputy H.M. Miles:

Thank you. You have talked quite a lot about your education prevention and safety by design. You said that you had reached a quarter of under-18s in your submission. Have you seen any concrete behaviour changes as a result of those sessions?

Information Commissioner:

That is probably a better question for the parents of those young people than for us. What we are seeing is far greater awareness of online risks and harms from young people than I think perhaps

most of us realise or give them credit for. Hence my earlier suggestion to make sure we involve young people in any collaborative initiative.

Deputy H.M. Miles:

How have you been doing that? How have you been engaging?

Information Commissioner:

What, with young people?

Deputy H.M. Miles:

Yes.

Information Commissioner:

Like I said before, through our schools, and we do surveys after each of the sessions and they have feedback that they provide us.

Deputy H.M. Miles:

If you have reached 25 per cent, what are your plans to get 100 per cent coverage on that?

Information Commissioner:

Just keep doing what we are doing, and attend as many secondary schools as possible. It is important to point out, we have one, sometimes 2, members of our team going around the schools. We are not flush with resource for that, but it is a continual piece of our evolving work trying to raise awareness of data protection and privacy as best as we can, and the law requires us to have a focus on young people. An even stronger focus is what we want our future society to look like, that is why our vision is built around creating a culture where privacy becomes instinctive. It is a long-term vision, 20 to 30 years ahead in the future. Providing the right tools and the right support for our young people now is a critical part of that vision and work as a regulator. There is a lot of good work going on with young people locally, not just with our office in terms of awareness raising and upscaling. For example, last week I was speaking to a local mediation firm who has been working with many Island schools on peer mediation, helping them to resolve conflicts and issues with friends, and they spoke about social media in particular a couple of weeks ago, and some of the difficulties that they were experiencing. I have brought a paragraph, I do not know if you will allow me to read it. This is a 10 year-old, and they said: "Sometimes social media can cause huge problems in today's world, and it is challenging communication between people, not always for the best. Children both in and out of school using social media do not understand the consequences of their behaviour and choices of words. Mediation in these circumstances can be difficult as children hide behind screens, or say a sibling has sent the message, not them, say it is just a joke or someone

has borrowed their phone. We feel that children and adults in and out of school appear to have 2 personalities. One is what you see is what you get, and the second is the internal emotions hurting inside and kept inside. Social media will always be a hard topic to resolve when issues arise. We would like to invite social media influencers to come and join us for a mediation session to see the destruction of people's lives in today's world." Now, if that does not speak to the understanding that a 10 year-old has in this arena, then I do not know what does.

Deputy H.M. Miles:

We have heard from C.Y.P.E.S. officers that they are developing online harm policies. We know that there has been a restriction on mobile phones in schools from September. What involvement has your office had in the development of those policies?

Information Commissioner:

We work with the Children's Commissioner quite regularly. We met recently with the Youth Advisory Group, which is just a small meeting, and that is helping us shape the questions and approach for a larger council meeting that is happening in November, and via C.Y.P.E.S. we are meeting with the School Council Network in November. We listen to feedback and comments from students when in in schools, and we get them involved in debates. We did a privacy debate 2 years ago, and hosted the Global Privacy Assembly Conference last year, which we had a group of Beaulieu students on stage. We do have a very good relationship with the relevant organisations. We were not directly involved in the mobile phone ban, and we have got some views on that.

Deputy H.M. Miles:

What views do you have on that?

Information Commissioner:

It is a step. It will be a mistake to say that it is going to resolve the problem, because it will not. A lot of the activities around mobile phone usage happen outside of school, and out of control of both parents and school teachers. I did see a comment in, I think it was, the *Jersey Evening Post* last week, which I entirely agree with, that we have got to be careful about giving all of the responsibilities to the parents and teachers in that world. The responsibility sits with the tech companies and providers. It is a difficult balance when you are looking at ... we came from an environment where we have learned to adopt technology into our lives. It did not exist when we were growing up. These are digital natives. They rely on these tools to be able to educate themselves, whether that is mainstream curriculum or whether it is current affairs or politics, or whatever it might be. So, to remove their ability to interact with that resource, it could be quite dangerous to them and place them at risk from exclusion. There are much broader issues beyond mobile phone usage in schools, and what they use it for, and it is difficult to control outside of that remit. But I do agree, and I do

understand the arguments that, yes, it is necessary because it is a control mechanism and it is ensuring that those children are kept safe.

Deputy H.M. Miles:

Thank you.

The Connétable of Grouville:

Regarding the proposed 48-hour takedown right, what elements do you think are essential for it to be both credible and workable?

Information Commissioner:

To be effective in the context of online harms and data protection, a takedown law must include clear enforceable mechanisms, like I said, that balance swift action with due process, and with clear respect to legal and jurisdictional boundaries. In order to work effectively, again, you need, firstly, a clear definition of what online harms is, specifically defining what constitutes harmful content, for example, cyberbullying, child sexual exploitation, doxing. It should distinguish between illegal content and lawful but harmful content to avoid overreach or suppression of legitimate expression. It needs to place obligations on online service providers, social media platforms, hosting providers and services to remove harmful content within 48 hours of receiving a valid complaint or notice, acknowledging receipt of that complaint immediately, and maintaining a report and an appeals process for users. There has got to be data protection safeguards included in there so that any takedown process respects the data rights of all individuals involved. So, including things like not revealing the identity of complainants unnecessarily, not processing data for longer than it is necessary, not holding data for longer than it is necessary, providing a clear record of decisions for accountability and audit measures. There has got to be user notification and rights of appeal. So, notifying the uploader if they are identifiable that their content was removed and why, and allowing an appeal process, allowing them to appeal the decision in ensuring fairness and due process, but a quick appeals process that can be resolved, say, within 7 days. Penalties for non-compliance will be needed, so that is imposing meaningful sanctions or other penalties; for example, restricting access or platform bans on platforms that fail to comply with requests on time. But providing as well for graduated enforcements of warnings first, then escalating up to penalties. Priority protection for children and vulnerable groups. So, fast track removal mechanisms for child-related harms, such as grooming, cyberbullying, image-based abuse, and urgent safety risks, so threats and self-harm content, and that kind of thing. Transparency and reporting. So, platforms will need to publish regular transparency reports showing the number of takedown requests that they have received, average response times, the number of successful appeals and removals, and then independent oversight. If this was a much larger jurisdiction, I would be suggesting the creation of an independent regulator or authority to handle complaints and disputes and unresolved cases, and audit

compliance, issue guidance on enforcement best practice. But Jersey is so small. Like I said, this function could sit well within the functions of my office but under a separate legislation that complements the data protection, provided sufficient resource, both human and financial, is forthcoming. To be effective, a 48-hour takedown law must combine speed, clarity and accountability and data protection principles.

[10:15]

It should empower users, especially children, to remove harmful content quickly while preserving fairness and legal oversight. The law must be capable of being enforceable. But also we could be really innovative and work together with tech companies rather than fight them. We are not going to change them. They are simply too powerful. Instead, we could work with them to make it a safer environment for children to navigate, place a responsibility on the tech companies to show young people themselves how to keep themselves online. Perhaps trial it across both Jersey and Guernsey in the first instance, and it could provide a good opportunity for Jersey to lead the way.

The Connétable of Grouville:

Commissioner, this Government had the opportunity to, I have often termed it “hook on to” the Online Safety Act in the U.K. via the permissive extent clause. In hindsight, would that have made your work easier or more difficult?

Information Commissioner:

I think it might have helped in certain areas. But because it is not really in our remit currently, I am not sure how we would know. In any case, it would definitely not be certain how well it would work until it had been in place for a significant period of time. The concerns we had, which I mentioned briefly earlier, that it does appear somewhat time-limited and it does not address emerging technologies such as generative AI or quantum computing, for example. Any legislation that relates to protecting people online needs to be future-proofed to be applicable to new, as yet unknown or untested, technologies and harms. Data protection law is a great example there. The privacy landscape has changed dramatically over the 40 years-plus that it has been around. But the basic principles of data protection have remained the same all the way through. So, perhaps a principles-based approach might be a good example to look at.

The Connétable of Grouville:

Thank you. How does Jersey’s commitment to E.U. adequacy sit alongside any future divergences in U.K. data protection standards?

Information Commissioner:

Any diversions from G.D.P.R. by a third country, which includes Jersey, in respect of the domestic law will essentially place their adequacy status at risk should the European Commission deem that divergence reduces the effectiveness in any way of individual rights. We are in a unique position here. For a country such as Jersey, our adequacy is absolutely fundamental to continued dataflows and trade, and therefore critical for our finance sector, which forms the basis of our economy. So, given adequacy is now assessed continuously, it is not just a rubber stamp and forgotten about, it is crucial that our data protection laws do not diverge from the G.D.P.R. The U.K. are already under significant scrutiny from the Commission regarding their own adequacy finding because of their proposed reform. We would not want to be in a similar position, and, again, hence my suggestion for a separate piece of legislation that complements data protection, or does not add to the existing framework.

The Connétable of Grouville:

Yes. Excellent. Emerging threats, such as deep fakes, are on the rise, as we all know. Are there additional tools or powers that would help J.O.I.C. address them?

Information Commissioner:

Deep fakes are just another form of technology, so the same tools or powers as would be required for any technology. Again, this is where principle-based approaches is really useful. Similarly, that is why any new law needs to be future-proofed and able to adapt to those new technologies, because they will change. If we legislate too narrowly then you risk excluding those emerging technologies and the resulting harms that might arise from the scope of the law.

The Connétable of Grouville:

Constant change, yes. Thank you very much.

Deputy C.D. Curtis:

Commissioner, looking 5 years ahead, what single change - legal, technical or educational - could make the greatest difference to children's online safety in Jersey?

The Connétable of Grouville:

There is a crystal ball right here, Paul.

Information Commissioner:

"What single change?" I think working collaboratively with the tech companies and social media platforms to help young people understand how to keep themselves safe online. We spend a lot of time as regulators and as jurisdictions fighting these big tech companies and it is futile. And I think you would agree to that, because you are not going to win. They are simply too powerful, too big,

and hold a lot of power in terms of market values and whatever. Are we going to be able to change it? No. So, rather than fight them, let us, for want of a better description, get into bed with them and let us get them on side and work with them. That is precisely why you would see, certainly from a global privacy assembly point of view, there is a big shift into having them involved, whether that be in terms of sponsorship or content, in terms of conference, because they are a big part of that conversation. If they are not involved in that conversation, then they are not going to learn anything from it, and neither will we. It is about that collaboration piece. It is about working together with them and trying to find a way forward that is going to be as great a benefit to the people that we are trying to protect.

The Connétable of Grouville:

Absolutely.

Deputy C.D. Curtis:

That could be the most realistic thing to do, but do think that they would be willing to work collaboratively?

Information Commissioner:

I think the tide is turning. Certainly they have been under a much greater degree of scrutiny in recent times than they have been previously. It is interesting, just from some of the conferences and meetings I have attended globally over the years, particularly I would say since 2018, since G.D.P.R. came in. You see some of these big tech companies will feed off each other. I remember the case, Microsoft, I think it was, that their chief exec at the time stood up in front of the Global Privacy Assembly and made a commitment to make their platform safer for young people. He was immediately followed by Mark Zuckerberg from Facebook, or Meta as it is now, and I cannot remember his name, but the then chief exec of Google, and they had no choice but to follow suit, because they could see which way the conversation was going. More and more over the years, you have seen greater involvement from those social media companies and the big tech companies wanting to do the right thing. I genuinely believe that none of them are deliberately attempting to harm children, no. The door is ajar, we have just got to open it a little bit further.

The Connétable of Grouville:

They cannot afford to step outside the circle.

Information Commissioner:

No. Correct.

Deputy C.D. Curtis:

Could you advise, as Commissioner, which indicators do you monitor, or plan to monitor, to gauge whether children are becoming safer online?

Information Commissioner:

Other than the work we do with the schools, we do not really measure online safety at the moment because it is not part of our regulatory remit. But, obviously, in the future if it did then we would put the appropriate measurement processes in place. We currently use outcomes-based accountability, a measurement model, which tracks with our approach of an outcomes-based, collaborative and regulatory approach. That is starting to play out and work now the data is being gathered. So, the same would apply in this context.

Deputy H.M. Miles:

Glad to hear it.

Deputy C.D. Curtis:

I know you gave us a lot of information already about a new takedown regime and how that is best done. How do you intend to share progress on that with the public?

Information Commissioner:

I think that is pre-supposing that there is a law in place that has a takedown provision, but in terms of sharing progress, the only way we would know is if the individual requesting the takedown had also notified our office. So, it depends how that mechanism works. If they have the ability to take it down themselves, we may not know. We will be wholly reliant on the providers to report those takedown numbers to us. But in terms of our own measurement model, we would have to be part of the reporting process for that to happen, which may or may not be something that we will.

Deputy C.D. Curtis:

While that is coming into place, assuming it does, you would publicise this to the public?

Information Commissioner:

Of course.

Deputy C.D. Curtis:

We are just at the last question, which is perfect timing. Lastly, is there anything the panel has not covered in its questions today that you feel would be important to mention regarding online harms?

Information Commissioner:

I do not think so. Just the opportunity to reiterate that any proposed legislation has got to be fit for purpose with practical enforcement capability that is future-focused so that it can easily be adapted to deal with new harms and technologies. We would strongly recommend a collaborative approach with all related and relevant stakeholders, and in particular young people involved in that discussion. But if there are 3 key takeaways for today, I would say, firstly, there is a decision to be made between legislation or some sort of voluntary arrangement with codes, or codes of practise, or age-appropriate codes. If we go with the legislation, then it needs to be very clear and consistent with other jurisdictions, because that interoperability is going to be key, particularly if you are doing overseas enforcement. Finally, privacy protection should sit at the core of any policy development in this area because of the quite significant overlap. I talked about corporate surveillance before, that will always be there, so privacy needs to be at the root of any legislative development in this area.

Deputy C.D. Curtis:

Well, thank you very much. That brings us to an end for this hearing. So, yes, thank you. That has been really interesting and very helpful.

Information Commissioner:

You are welcome. Thank you.

[10:26]