DÁIL ÉIREANN

AN COMHCHOISTE UM DHLÍ AGUS CEART AGUS COMHIONANNAS

JOINT COMMITTEE ON JUSTICE AND EQUALITY

Dé Céadaoin, 5 Iúil 2017

Wednesday, 5 July 2017

Tháinig an Comhchoiste le chéile ag 9 a.m.

The Joint Committee met at 9 a.m.

Comhaltaí a bhí i láthair / Members present:

Teachtaí Dála / Deputies	Seanadóirí / Senators
Colm Brophy,	Frances Black.
Jack Chambers,	
Clare Daly,	
Jim O'Callaghan,	
Mick Wallace.	

Teachta / Deputy Caoimhghín Ó Caoláin sa Chathaoir / in the Chair.

General Scheme of the Data Protection Bill 2017: Discussion (Resumed)

Chairman: Apologies have been received from Deputy Alan Farrell. I ask everyone to please switch off all mobile phones as they interfere with the sound recording system.

The purpose of today's meeting is to conclude our pre-legislative scrutiny of the general scheme of the Data Protection Bill 2017. We have two tranches to our sitting today. The first of those will address points to be raised. I extend a warm welcome to Dr. T.J. McIntyre, a law lecturer in UCD and chair of Digital Rights Ireland, and Mr. Simon McGarr, solicitor. On behalf of the committee, I thank them for their attendance here today and apologise for the slightly late start of our business. The format of the meeting is that they will be invited to make an opening statement, which will be followed by a questions and answers session.

I remind those present of the situation with regard to privilege. Witnesses are protected by absolute privilege in respect of their evidence to the committee. If witnesses are directed by the committee to cease giving evidence on a particular matter and they continue to do so, they are entitled thereafter only to a qualified privilege in respect of their evidence. Witnesses are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable.

Members, while they probably know it off by heart at this point, should be aware that under the salient rulings of the Chair, they should not comment on, criticise or make charges against a person outside the House or an official by name or in such a way as to make him or her identifiable.

I invite Dr. McIntyre and Mr. McGarr to make their opening statements.

Dr. T.J. McIntyre: I would like to make four points today on behalf of Digital Rights Ireland. First, I thank the committee for the opportunity to discuss the Bill. This is an area of law of immense importance and the decisions taken in implementing the general data protection regulation, GDPR, will be in place for many years to come. After all, it is now nearly 30 years after the 1988 Act came into effect and I suspect we will see this in place for something close to the same time.

The first point I would like to make is on the structure of the Bill. I know that previous witnesses have said the Bill is over-ambitious in that it tries to do much in one document, and I agree with that. In particular, it would be desirable to separate the provisions the Bill, specifically in Part 4, which implement the law enforcement data protection directive and place them in a separate instrument. This is because there is a significant overlap, or at least a perceived overlap, between the two areas. I have already seen a degree of confusion on the part of people reading the heads of Bill who have read a section in Part 4 that appears to be reflecting the general data protection regulation, GDPR, when it is not implementing it but rather the directive. There is a real risk that the very similar language will lead to a degree of confusion on the part of users.

The other point made by previous witnesses, in particular the commissioner and Mr. Denis Kelleher was that the residual Parts of the 1988 and 2003 Acts should be repealed and re-enacted as a stand-alone instrument rather than being left in place. I support that argument. It seems that if we leave any Parts of the 1988 and 2003 Acts in place, we will have a position where to deal with certain matters, in particular those with an overlap between public and private processing of data, we will have to look to the 1988 Act, determine how it was amended by the 2003 Act, determine how that was amended by what would be the 2018 Act and then look to the GDPR on top of that, possibly while looking to other European instruments on top of that as well. For example, these might include European instruments regarding the Schengen information system. It seems that would be a real recipe for confusion.

It would be greatly preferable to deal, as far as possible, with the few aspects remaining in the 1988 Act in a short, separate and stand-alone instrument. These are the aspects required of Ireland under the 1981 Council of Europe privacy convention but not dealt with under the GDPR or the law enforcement data protection directive. This is something we will have to do in any event. The Council of Europe convention on the protection of personal data is in the process of being modernised and we are at a point where we are very close to agreement on a final text. This is something that will be implemented certainly in the next couple of years in any event. It would be very useful at this point to pre-empt that as far as possible by separating those provisions.

The next point relates to article 80 of the GDPR, which deals with representation of data subjects. A real problem in this area has been that individuals can lack the expertise, knowledge, time and money to enforce their legal rights. As members know, the Irish legal system is expensive and difficult to navigate for lawyers, never mind those people unfamiliar with it. Many of these rights, if they are to be enforced, would involve a trip to either the Circuit Court or the High Court at a cost that is simply beyond the scope of the average individual. The GDPR aims to alleviate that problem with a mandatory provision and two optional provisions in article 80. The mandatory provision is that member states must allow individuals to nominate a not-for-profit body to act on their behalf to make complaints to a data protection authority, appeal against decisions of a data protection authority, or take an action against a controller, like an Internet service provider, where it has abused personal data. The optional parts of the article are that member states may allow individuals to nominate not-for-profit groups to act on their behalf to seek damages and they may allow not-for-profit groups to bring actions on their own initiative without the need for an individual to nominate them to do so.

It is very important that Ireland would take up the two aspects of flexibility in the GDPR and it is rather disappointing the heads of Bill do not address these points at all. The heads of Bill before us now would exercise the discretion silently that would not take advantage of these options. There are practical and principled reasons it would be useful to make these changes. The practical reason is that given Irish law does not allow for class actions, as such, and there is no general provision for them. If individuals are not able to nominate a representative body to bring an action for damages on their behalf, there will be a multiplicity of claims being brought before the courts that the courts simply are not equipped to address. One might think about a data breach, for example, such as the Yahoo compromise or the Ashley Madison data breach, where there could be thousands, tens of thousands or hundreds of thousands of individuals affected, some of whom may be very seriously affected. In that context we can expect a similar number of cases coming before the courts. The GDPR gives us the option to effectively consolidate these cases if we allow people to nominate not-for-profit bodies to act on their behalf to bring a single action. Without that option - it is not an option under the heads of Bill as they

stand if individuals are seeking damages - the individuals, if they have time, expertise and knowledge to bring an action individually, will have to do so individually.

The second reason is a principled one. It seems that if individuals are not able to nominate not-for-profit bodies to bring an action for damages on their behalf, and if not-for-profit bodies are not able to bring an action in appropriate cases where an individual complainant has not come forward, there will be a gap in protection. In many cases, in particular discussing sensitive personal data, individuals - even if they can be identified and know they have been harmed - would be very reluctant or unable to come forward. Individuals who find sensitive medical records leaked, for example, or, like with the Ashley Madison case, those who find information relating to their sexual life has been leaked would be very often unwilling to become the public face of the issue for very understandable reasons. Although we might be able to identify an affected individual, that is not to say the individual would be in a position to bring a complaint or action in respect of the matter.

This is important from a principled perspective because, in our own litigation challenging data retention law, Mr. Justice McKechnie in the High Court acknowledged that it was important that Digital Rights Ireland would be able to bring an *actio popularis*, an action on behalf of the wider population in respect of data retention laws. This was a pressing issue of public concern and if we were not able to do it, individuals would not have the financial ability to bring the action by themselves. In an area where the European Union was eventually found to have acted in a manner that was entirely illegal, this would have gone unchallenged because individuals simply did not have the resources to bring these claims. As members will know from a number of hearings, this is an exceptionally complicated area of law. We say it is unrealistic and unfair to expect individuals to navigate these waters without a guide. The two discretionary provisions in article 80 are necessary to enable individuals to have an effective remedy.

My next point does not appear on the speaking note that was distributed but it relates to head 20 of the Bill, which would allow for restrictions to be placed on controller obligations and the exercise of data subject rights by means of statutory instrument. We are concerned that head 20 appears to introduce a far-reaching power on the part of each individual Minister to effectively exempt particular forms of data processing from the requirements of the GDPR in a way that might not be fully consistent with fundamental rights. It is noticeable that in the heads of Bill the Department acknowledges it would be desirable for Departments to introduce limitations on these rights by means of primary legislation but it suggests it is nevertheless necessary to have a residual power by means of statutory instrument to introduce these exceptions.

This power, certainly as drafted in the heads of Bill, goes significantly too far. In head 20, subhead 2(s), there are two typographical errors but the second is the one to which I refer. It states that a statutory instrument may be introduced which will restrict controller obligations and data subject rights in relation to important objectives of general public interest. What are such objectives? They are defined in head 20, paragraph 2, under the second subsection (s) as "such other important objectives of general public interest of the Union or the State as may be prescribed in regulations". In other words, we may have regulations introduced where necessary for matters of important general public interest. What are matters of general public interest? They are matters which may be defined by the regulations to be introduced to implement matters of general public interest. Even in that aspect of the heads of the Bill there is circularity in the definition.

More generally, there is a concern that we are creating a very far-reaching power to carve out exemptions from the GDPR without clear standards being laid down in legislation to do

so. It seems to me that if such a far-reaching power is to be in place, there should be some additional check on it. What that check might be is a matter for the Oireachtas. It could be a requirement for a positive resolution of the Houses before the exemption would come into effect. It could be a sunset clause whereby any regulations introduced under this provision have a finite lifespan and must either be re-enacted in primary legislation or allowed to expire. It could be some other mechanism for parliamentary or perhaps committee scrutiny of particular classes of regulation. As this stands, however, particularly in the context of a minority Government, there is a risk that exemptions could be introduced by ministerial order which might not pass full legislative scrutiny and certainly might not command the support of the Houses of the Oireachtas.

I apologise that my final point is not included in the speaking note provided to the committee. It concerns the position of data protection officers, DPOs, and the protection they have if they are victimised for doing their work. As the members know, under the GDPR data protection officers are required to be independent. Data controllers are not to interfere with the independent exercise of their functions. However, the remedies available for breach of this duty are sanctions imposed by the data protection authority on the data controller. They are not remedies that are available to the data protection officer who might have been victimised as a result. For example, if an individual DPO is sacked for doing his or her job, there is no remedy available to him or her under the GDPR itself or under the heads of the Bill. It seems to me that it would be desirable to provide some form of remedy.

DPOs already have recourse to a limited form of remedy in that they might have the right to bring an action for wrongful dismissal. As committee members will be aware, however, an action for wrongful dismissal is a limited one in the sense that it is quite expensive. It must be brought before the Circuit Court or High Court as appropriate. It would be preferable to provide that DPOs have available to them an action for unfair dismissal, which is a much cheaper, easier, streamlined process that can be brought before the Workplace Relations Commission and the Labour Court.

The analogy here would be to the Protected Disclosures Act, which creates a protection for those who are dismissed on the basis of protected disclosure. There would in fact be an overlap in that, in some cases, DPOs might make a protected disclosure precisely in order to bring themselves within the scope of that legislation, for example by notifying a matter to the Data Protection Commissioner. It would be preferable to avoid the need for them to artificially bring themselves under the purview of the Protected Disclosures Act by explicitly providing that, where an individual is dismissed on the basis of the exercise of his or her functions as a DPO, an unfair dismissal remedy would be available to him or her.

That concludes my statement on behalf of Digital Rights Ireland. I welcome any questions.

Chairman: We will take both opening statements first and questions afterwards. I thank Dr. McIntyre for his very informative contribution which expanded on the points he had already provided to us. I now invite Mr. McGarr to make his opening remarks.

Mr. Simon McGarr: I thank the committee for the opportunity to address it on the heads of the Bill. This legislation, together with the implementation of the GDPR, will mark a watershed in respect of the relationship between the State and its citizens. I will address three major points and will pick up some of the threads from Dr. McIntyre's submission.

First I will address head 23, a proposal in respect of State agencies, public bodies and administrative fines. It provides for administrative fines to be imposed on public bodies or

authorities solely in respect of occasions on which they act as an undertaking. The effect of this exemption is to make sure they are not liable to fines on all other occasions when they are not acting as an undertaking. The result is to exempt public bodies and State agencies from administrative fines. The committee will have heard from the Data Protection Commissioner and other witnesses already. I echo them in saying that this is a very unwise course of action for the State to have taken.

State agencies will not have the same level of accountability as commercial bodies. Between State agencies, a tally in respect of fines over the course of years is a very good initial indicator of any structural or institutional difficulty that may be arising. Such a difficulty is easy to see as the fines build up, should there be repeated fines, and therefore it is less likely that long-term structural difficulties will develop. Administrative fines are cost-neutral for the Exchequer as a whole. The fines levied on public agencies go back into the Central Fund. There is not really a cost saving exercise here for the State or the Exchequer.

The proposed provision requires a legally very complex test to be carried out on each occasion that the data protection commission thinks it is necessary to do so, before any administrative fines could be levied. On every occasion, there would have to be an examination of whether elements of public authority were acting as an undertaking before an administrative fine could be levied. In the explanatory note to the heads of the Bill, it is acknowledged that this is a complicated matter. It cannot be said that a particular State body is an undertaking in all its activities. The example given in the explanatory note is that the HSE in the provision of ambulances is sometimes an undertaking and is sometimes not. This is a high legal threshold for the regulator to have to get over every time it must decide whether it is possible to exercise legal powers. It also introduces the potential of a challenge by the public body to every such effort to exercise those powers, in respect of whether it is acting as an undertaking.

It seems that there is very little by way of compelling reasons for providing this exemption for the State bodies. Certainly there is nothing set out in the explanatory note as to why State bodies ought to be exempt as a matter of policy. There are very clear reasons for having State bodies subject to the same regulatory system as the rest of civil society. Our recommendation is that it would be better if article 83(7) was implemented without any restrictions on the administrative responses available to the Data Protection Commissioner, including such fines as the commission found appropriate in respect of breaches of citizens' personal data privacy. Head 91 deals with the requirement giving effect to the GDPR provision that there should be a right of compensation for financial and non-financial loss arising from a breach of the regulation. Article 82 of the regulation is phrased in such a way as to say that there "shall" be provision made for the recovery of compensation for material and non-material loss. The wording of the article is such that precedent would suggest that, when a European legislative provision states there shall be provision, it indicates that a further step is likely to be necessary on the part of the member state in order to give force to that intention.

The heads of the Bill recognise there is a right of action but on examination it does not explicitly create a right of compensation of data subjects for a breach of their rights. The result would be that there is a question whether the State would have complied with the requirement that there shall be a provision for the recovery of compensation.

This has unattractive features from the point of view of potential data subject citizens where there might have been a breach of their rights. It will also leave the State open to potential claims from people who find that they were unable to enforce their rights as it is a requirement under European law if a person has not been able to recover the compensation that should have

been provided for under European law, as a result of a failure by the State, that per the Frankowicz case they have a right to recover such damages as they would have recovered from the third party from the State. The result is that, by not implementing an explicit statement saying that there is a right of compensation as opposed to a right of action, the State may hold itself open to any of the damages that would have otherwise fallen on private third parties who were breaching the data protection rights. For all those reasons, we recommend that it would be better to see the intent of Article 2 of the regulation and Article 56 of the directive being made explicit by way of an explicit legislative recognition of the right of recovery of compensation for both material and non-material damages.

Dr. McIntyre has dealt with the separate implementation of regulation and directive but I would like to add that the current general scheme of the Data Protection Bill seeks to do three separate things: to largely, but not completely, replace the existing Data Protection Acts under head 5; to legislate for a small number of matters in the GDPR which have been left to member states such as the Internet age of consent and other matters; and to transpose, entirely by way of part 4 of the heads of Bill, Directive 2016/680 in respect of national security. We do not think it is a good idea to attempt to do those three things because this legislation must be passed and it is on a deadline. The GDPR comes into force in May of next year, and by running the implementation measures in respect of the GDPR together with the complicated matters in transposing a directive and the partial repeal of the data protection Acts, we run the risk from a practical point of view of either legislative gridlock preventing the matter from progressing at the required speed, or of the matter passing without the necessary scrutiny in respect of one area of the Bill because there is such a pressing deadline in respect of other areas. For those reasons, we recommend that it is better to address the transposition of Directive 2016/680 by way of a specific legislative instrument separately. This would allow any of the necessary residual elements required from the data protection Acts for that transposition, or as a result of the requirements of the State as a member of the Council of Europe, to be dealt with separately in another issue. This would then allow for the full repeal of the existing data protection Acts which are intended for partial repeal under head 5 and their replacement by the GDPR in Irish law.

We think it would be a good idea if the GDPR is reproduced as either an annexe or appendix verbatim in the final Bill, together with a few domestic legislative variations which are provided for under the regulation. As well as providing clarity for users and the courts in the consideration of what is quite a complex area of law – I am sure every lawyer says their pet subject is a complex area of law but I hope the committee will agree that this one does seem to meet the bar for that description - but it also significantly reduces the chance of any legislative uncertainty as to what provisions are being applied by the court at any given moment. Therefore, the likelihood of challenges to the interpretation by the new data protection commissioner before the courts is reduced. That is a valuable aim in itself. The data protection commission, which is set up, will be a new body exercising significant new powers and it is important for building up confidence in that body, but also in respect of the courts relationship with that body as a place of appeal from its decision making, that exactly the laws it is working under and exactly the powers it is implementing are as clearly set out by the Oireachtas, in advance of the commencement of the commission in order to allow the commission to fully exercise its rights without the fear of constant challenge, which we have seen in previous regulatory systems that have been introduced. Particularly where large amounts of financial administrative fines are at stake there is an incentive for judicial challenge. That is always available for people to take and if bodies or individuals feel they have not been treated properly by the data protection commission, it is right that they should be able to take the matter to the courts. We are suggesting, however, that in order to make sure that those appeals are minimised, it is best that the law the decisions are

taken under is as clear as possible for all users.

I want to deal with a couple of matters that Dr. McIntyre has raised, specifically the exemption carved out to give the Ministers powers to effectively grant an exemption to anybody on any matter they think relevant. I think that is under head 20. This is a matter that has been live before the European courts in recent years. In 2015, the Bara judgment dealt with a data sharing provision by the Romanian Government on foot of legislation which the Court of Justice of the European Union said was not acceptable on the basis that it had shared this data between two government agencies and that doing this without the prior knowledge of the data subjects was contrary to the charter of fundamental rights and the data protection directive. This is significant because it means that, even when the matters are provided for by legislation, the State does not have a free hand to pass any such legislation that it wants to in order to carve out exceptions from a matter that is underpinned by the charter of fundamental rights. In passing any such exemptions, it must give consideration to the questions of necessity or proportionality.

The heads of the Bill take no account of these limitations on the national member state's executive powers. They deal with a very wide range of stated bases and a general catch-all unstated basis on which these powers could be exercised, including such things as maintaining registers for reasons of general public interest. This seems to be a general right to build databases in respect of the population. Whether these provisions, if they were passed into legislation, would pass scrutiny before the Court of Justice of the European Union I could not say for sure, but certainly some provisions that are foreseen as being carved out by head 20 would fall foul of the same legal arguments that struck down the Romanian legislative provisions on data sharing. I know the data protection commissioner has issued a guidance note to State agencies on data sharing following the Bara judgment and the State has received guidance from its legal advisers in respect of the desirability of passing such data-sharing exemptions from the data protection directive by way of primary legislation. It is important that if the State is to provide for certain matters to be dealt with and if primary legislation is required in order to ground an exemption from the data protection directive on a lawful basis, which is provided for in the directive, it should not provide for non-primary legislative means. It seems like a recipe for challenge and, in all likelihood, a recipe for the data protection commissioner to have to deal with a repeated number of complaints and challenges to actions of the State. There have been recent examples in respect of the primary online database where certain databases were rolled out with very long or indefinite retention periods involving holding the data of five year olds indefinitely and those matters have had to be rolled back following the engagement with the Data Protection Commissioner as to what was and was not appropriate under European law. I do not think we should allow for an unqualified right of a Minister to provide for exemptions from European law at the stroke of a pen by way of a statutory instrument regardless of whether that is attractive to the Executive as a method of providing for regulatory activity. It should be the case that we should go by way of primary legislation if there is to be a reliance upon the lawful basis exemptions from the data protection directive. That is all I wanted to say on that matter.

Chairman: I thank Mr. McGarr and Dr. McIntyre for their contributions and their written submissions.

Deputy Jim O'Callaghan: I thank Mr. McGarr and Dr. McIntyre for attending the committee meeting. Listening to both of them and their views as to what areas in the legislation could be improved has been informative. I will make a few comments about the structure of the Bill because both Mr. McGarr and Dr. McIntyre raised it. They are correct in stating that it would be preferable if the 1988 and 2003 Acts were repealed in order that people who want to

know what the law on data protection in Ireland is could come to one new piece of legislation and see it there rather than have to go back to legislation from 14 years ago and from 1988. I had not been aware of the potential for confusion that can arise from the inclusion of Part 4. There may be logic in trying to separate the GDPR legislative basis from the other one. That is really a matter for Government. It will be difficult for us to do that as a committee by way of an amendment, but it is an interesting point and something to which I will give further consideration.

In respect of the point made by Dr. McIntyre about the representation of data subjects, I would have thought there is a legitimate concern on the part of data controllers, the Oireachtas and Government that this could become an overly litigious area. While there are people who have minor data breaches and who are perfectly entitled to have them ruled upon, there could be a concern on the part of the Legislature or Executive that it will involve lawyers taking cases, and even though there is minimal compensation to be paid, it will result in a lot of costs. I can understand why that is a legitimate concern.

I am interested in the reference to the non-profit entities. I looked at the definition of a non-profit entity in Article 80. Will the witnesses provide us with further explanations? What would be a non-profit entity in an Irish context? Obviously, Digital Rights Ireland would probably be one. Will Dr. McIntyre give us other examples?

Dr. T.J. McIntyre: Yes. In fact, Digital Rights Ireland might not be the best example because I would envisage that this is an area where there might be consumer rights groups bringing actions. I believe this is common in Germany. Data protection rights are an aspect of consumer rights, and if a consumer rights body is active in the area of the protection of consumer privacy, there is no reason it could not bring an action. I would envisage that trade unions might fall into that category as well if they are protecting the privacy of employees at work. The National Union of Journalists might fall into that category if it was protecting the privacy of journalists from surveillance by the State. It seems to me that it would not be limited to traditional civil rights groups but has a wider application.

The Deputy's point regarding the possibility of burdensome litigation is a fair one. However, it is one that has already been addressed to a large extent. The existing provisions deal with that. The fact the Data Protection Commissioner has the discretion not to entertain claims that in current language are termed "frivolous and vexatious" represents an important safeguard that is already in place. One can add to that the requirement there be a filter here. The provision that only qualifying non-profit entities get to bring these actions is an important one. I do not think many bodies would be set up with these objectives and have this track record. It is ultimately open to the court to decide if the particular body qualifies.

Deputy Jim O'Callaghan: Does that mean Dr. McIntyre probably thinks it would be broader than the way I described it? It would not be groups set up purely for data protection purposes. It could be representative organisations, trade unions and other bodies that are interested in protecting their members and that are not in the business of making profit.

Dr. T.J. McIntyre: Based on the German experience relating to consumer groups, I would say "yes". It is not like digital rights groups in Ireland are so well financed and well equipped to bring these actions.

Deputy Jim O'Callaghan: Is Digital Rights Ireland's complaint that it thinks that these representative, not-for-profit bodies should be permitted to seek compensation as well as decla-

rations in respect of the persons on whose behalf they are taking actions?

Dr. T.J. McIntyre: That is right. It is compensation on behalf of the data subject. It is not something that would be funnelled into the coffers of a particular group. Without the ability to seek compensation, we give individuals what is to my mind a very unfair choice. They have suffered loss as a result of, for example, a data breach. They can either seek a remedy by going through a non-profit group but give up the right to damages or they can seek damages but only if they have the knowledge and financial resources to bring the action and they must put themselves at risk of bearing the costs of the other side if they lose the action.

Deputy Jim O'Callaghan: Both Dr. McIntyre and Mr. McGarr made a point about head 20 and the general public interest. I agree that it is not particularly well drafted, although it is drafted extremely broadly. There is a standard legislative mechanism that can be included whereby it says that any order under this provision must be placed before the Houses of the Oireachtas and can be voted down within a period of 21 days. Do the witnesses think that would be a suitable mechanism for dealing with their concerns?

Dr. T.J. McIntyre: Is the Deputy suggesting the standard negative resolution procedure?

Deputy Jim O'Callaghan: Yes, that it would be placed before the Houses of the Oireachtas, and unless there is a resolution voting it down within 21 days-----

Dr. T.J. McIntyre: I am not sure this would suffice as a matter of European law. I question whether head 20 as it stands would fit the test regarding whether the powers are sufficiently clearly set out to begin with. It seems to me that especially some of the latter provisions, namely, the important objectives of general public interest and open-ended discretion as to how they are to be protected, might not even meet domestic constitutional standards.

Deputy Jim O'Callaghan: Dr. McIntyre is saying it is far too broad and provides too many parameters to the definition of general public interest?

Dr. T.J. McIntyre: It is trying to do an awful lot in the sense that it is giving these powers to any relevant Minister to do any of these things in the context of any of these interests and, of course, it is cutting back on the scope of a fundamental right protected by the EU Charter of Fundamental Rights.

Deputy Jim O'Callaghan: Dr. McIntyre's fourth point concerned a data protection officer who may be victimised. I think the witnesses want a specific statutory protection for that officer in the legislation. Will Dr. McIntyre give me an example of the type of victimisation he is talking about? When I first heard him say it, I thought that surely there would be a standard remedy in terms of going to court, be it for wrongful dismissal or something else. Could an individual not pursue an action for wrongful dismissal as well as it stands at present?

Dr. T.J. McIntyre: The Deputy may be able to correct me but I do not think this would be a protected category under which an unfair dismissal action could be grounded unless someone was artificially to turn it into a protected disclosure by taking the concern to the Data Protection Commissioner and then saying he or she was being penalised on the basis of a protected disclosure.

Deputy Jim O'Callaghan: Under the protected disclosure legislation, is it the case that if someone goes down the unfair dismissal route, his or her remedies are greater than they are under the standard unfair dismissal route? Is is true that the person can claim up to five years'

wages as opposed to two years' wages?

Dr. T.J. McIntyre: I do not have the Act in front of me.

Deputy Jim O'Callaghan: Mr. McGarr made the point that there should be explicit legislative recognition of the right to recovery for compensation because, without it, people may not be aware of their entitlement to seek it.

Mr. Simon McGarr: More significantly, I said that not only might they be unaware of the right, the State may not have provided for that right if there is no explicit recognition. As it is drafted, there is an explicit recognition of a right of action but it does not necessarily follow that there is also a recognition of a right of compensation. The GDPR provides only that there shall be - future tense - a right of compensation provided for. It seems to me that the intent of the State clearly is not to fall foul of European law. It does not intend to try to remove people's right of compensation and therefore it would be better that we explicitly include that right, which is addressed in the GDPR, in that head.

Deputy Jim O'Callaghan: It may be the case that even if it is not in it, people would still have the right to seek compensation, but does Mr. McGarr think it is preferable to have it included in any event?

Mr. Simon McGarr: That is arguable because there are other instruments in European law where there is a requirement that compensation shall be provided. That requires a further step by the member state to give function to that intent.

Deputy Jim O'Callaghan: I note the point that Mr. McGarr makes about head 23, something I mentioned to Mr. Denis Kelleher when he was giving evidence before us. Mr. McGarr is concerned that in regard to the undertaking, the State is trying to apply a different standard to itself than applies to other data controllers.

Mr. Simon McGarr: Yes. Let us leave aside the active provision that the State shall be liable for fines when acting as an undertaking. The result of that positive statement is to create, although unstated in the head, a requirement that the State shall not be liable under any other circumstances. There is no justification provided for in the heads of the Bill that we can examine and address, but it certainly does not seem to me that it would be in line with best policy practice to allow the State to exempt itself from the provisions of what are very significant citizenry rights protection legislation.

Deputy Jim O'Callaghan: I thank Mr. McGarr.

Deputy Mick Wallace: I thank the witnesses for coming before us. It is important to acknowledge that the witnesses know more about this issue than we do. I cannot help thinking that the witnesses know more about it than the officials who are drafting this Bill. Have the witnesses had any meetings with those drafting the Bill or have they consulted the witnesses?

Dr. T.J. McIntyre: Only informal meetings. There has been no formal input. I do not think there was any formal public consultation regarding this Bill. There may have been some on the digital age of consent, but I do not think there was any formal consultation otherwise.

Deputy Mick Wallace: Last year, Digital Rights Ireland commenced legal proceedings against the Irish State, challenging the independence of the commissioner and alleging that the commissioner did not effectively monitor databases containing personal data that had been cre-

ated by public bodies. Also the fact that the commissioner is integrated into the Department of Justice and Equality and that many of the employees of the office are civil servants may raise questions about the independence of the office. Are the witnesses happy with the level of independence the Data Protection Commissioner is likely to have in future?

Dr. T.J. McIntyre: The litigation is pending so it would not be appropriate for us to get into that in this forum.

Deputy Mick Wallace: It is funny. I have heard that before.

Chairman: A very wise response.

Mr. Simon McGarr: He is acting on the advice of his lawyer in answering in that way.

Deputy Mick Wallace: A report carried out last year by the International Network of Civil Liberties Organisations, INCLO, called Surveillance and Democracy: Chilling tales from around the World, highlights the dangers of secretive international information-sharing agreements between intelligence agencies along with the problem of domestic surveillance. There are reports of people being put on secret fly lists, based on harmless email exchanges, state security agencies using intimidation tactics against peaceful protesters and national surveillance databases containing sections dedicated specifically to human rights activists. There are concrete cases of where individuals' human rights have been violated by the state. In light of the recent moves to introduce a national identity card and the potential to put so much information on this card, obviously we are aware of the fact that a lot of information can also be put on our passports. The data protection commissioner is on record as saying that, with regard to identity cards, the individual concerned has a right to know exactly what data are recorded on the card. Would Mr. McGarr accept what I have said as valid?

Mr. Simon McGarr: On the specific question in respect of the public services card, it does have a great deal of the appearance of a national ID card scheme in its scope, and that scope is increasing regularly to the point that one is no longer able to apply for a driving licence for the first time without having a public services card. People who are applying for their first passport must first take up a public services card. That is a subsection of a wider question, which is relevant to the Bara judgment, which is that the State has taken many concrete steps in recent years to build not merely an ID database of which the public services card is the physical manifestation but also a series of national databases intending to capture not merely all citizens' data but also data on people travelling through the State by way of the passenger name recognition database, PNR, and on all residents, who may not necessarily be citizens, of course, by way of the individual health identifiers database. On each occasion that these steps have been taken, provision has been made to take the data which has been collected from individuals by other agencies for other purposes and apply it to this new purpose, this data-sharing between bodies. This is again exactly the matter that was before the Court of Justice of the European Union, CJEU. It is again exactly the matter in which the Romanian Government was found to have acted unlawfully in transferring its data between its equivalents in Romania of our Department of Social Protection and Revenue Commissioners. It seems to me that, despite the data protection commissioner producing an excellent briefing note for the State on these matters, there has still been, shall we say, Executive reluctance to absorb fully the lessons of what European law states on the limits of state data-sharing.

Nonetheless, what we can see here and in other recent proposed legislation, including the proposed data-sharing Bill, is that there is an effort by the State to continue to provide a back-

stop for its projects that are under way and on which a great deal of money has been spent while at the same time not fully addressing head-on the question of citizens' rights in respect of data-sharing. That is not an attractive way for the State to have acted. In particular, notwithstanding the very legitimate reasons there may well be, for example, in the health sphere, for creating databases which can contribute to public safety and to health safety, the level of trust that is required to allow databases of that sort to be built must be built first on the understanding of the citizenry as to what is being done and must be built up in order that they know it is being done in the right way and that they trust it is being done in the right way. Internationally what we have seen is that, if trust is not built first and there is an administrative push to collect the data and explain it to people later, very expensive and substantial projects fail completely. I am thinking of the NHS care.data project, which was a centralised health records scheme that failed completely after the expenditure of million of pounds sterling in the UK as a result of a basic failure of public trust in how the data were going to be managed. I am thinking of the Australian identity card scheme and public identity register which effectively came to a creaking halt once the Australian people lost trust in the scheme as it was being provided for.

These matters are not tidying-up matters. It is not a matter of going back and explaining it to people afterwards. If trust is not built into the scheme from the start, the necessary explanations cannot be provided, and people do not think their legal rights to their data privacy are being respected, potentially very valuable public schemes become hamstrung from the very start. It is not merely counterproductive from an administrative point of view and in terms of the loss of time and money; it is also very destructive of the relationship between the state and the citizen.

Deputy Mick Wallace: On that same theme, does the new legislation square with the ongoing health identifiers framework project which aims to have a database in place which will track every Irish citizen through the health service from birth to death? The legislation underpinning the project, the Health Identifiers Act 2014, allows for Ministers from various Departments to share data about individuals with the Minister for Health for the purpose of this database. It appears to be in direct violation of the case law of the EU court. As the health identifiers project was initiated before the Bara judgment, questions arise about whether it has been scrapped in light of the legal implications of that judgment. If not, what measures are in place to ensure any data-sharing can only be done with the permission of the individual?

Dr. T.J. McIntyre: I agree with the Deputy's points in that regard. When the scheme was first mooted in 2008, the Department of Health promised that the individual health identifier would be introduced on an opt-out basis, which meant people would be able to choose whether to participate in it. There was never any explanation of why that commitment was later abandoned.

Deputy Mick Wallace: Right.

Mr. Simon McGarr: I have submitted some freedom of information requests relating to the individual health identifier project. It seems to me that there has been a rush to bring the project through. Following the Bara decision, there was an acknowledgment that further advices needed to be taken to ascertain what its consequences were. Regardless of what those advices might have been, there has been no hesitation, pause or slowdown in the implementation of the plan that was previously outlined. It seems to me that the right to compensation which has been introduced in the GDPR cannot be removed by individual member states, even if the administrative fines element is left in. On the question of whether the State is causing itself difficulties, I would argue that following the Bara judgment the Health Identifiers Act does not comply with European law. If this turns out to be the case following the decision of the court,

there will be grounds for a claim of compensation for actual financial loss or for non-material loss. Every single resident of the State - one will not need to be a citizen - will have a claim on the State in such circumstances. Regardless of whether a resident has a financial loss as a result of the breach of his or her rights, he or she will have a right to compensation for non-financial loss. The risk that the individual health identifier database poses to the Exchequer and to the relationship of trust between the State and its citizens is such that it would be very valuable for the matter to come under extremely close scrutiny between now and the implementation of the GDPR in May 2018. It seems to me that the approach taken by the HSE, and perhaps to a lesser extent by the Department of Health is that because this matter has been legislated for, it intends to carry on until someone tells it to stop. I am not sure whether that is the best way to deal with an extremely complicated matter where European law is moving forward and changing the grounds on which the risk assessment would be made.

Deputy Mick Wallace: When I asked the Data Protection Commissioner about the information gathered by phone companies, she told me there is no specific provision under the Communications (Retention of Data) Act 2011 that obliges her office to notify a person about whom a request has been made for access to his or her telecommunications. We have been communicating with the phone company 3. According to a reply we got the other today, when the company receives requests from data subjects equivalent to requests which had been made, it considers that such requesters do not generally have a right under section 4 of the Data Protection Acts 1988 and 2003 to data about information requests received by it from State agencies which the company may possess. What do the witnesses think of that?

Dr. T.J. McIntyre: There are two issues here. The first issue is the standard in Irish law under which surveillance can be carried out. The standard in Irish law at the moment is that surveillance can be carried out on someone by ministerial warrant in the case of listening to his or her phone calls, and by individual internal Garda authorisation and signature in the case of accessing his or her phone records. Following the recent judgment of the Court of Justice of the European Union in the Tele2-Watson case, I think it is reasonably clear that this is inadequate. The judgment in question makes it clear that there must be judicial authorisation of surveillance in the case of accessing phone records and - all the more so, it seems to me - in the case of listening to phone calls. The second issue is important as well. In the Tele2-Watson case, the court went on to say that, in addition to having prior judicial authorisation before phone records can be accessed, there must also be some form of after-the-fact notification. In other words, the person whose phone records were accessed must be notified of that at a later stage - after the investigation has been concluded - as long as he or she can be notified without undermining a law enforcement purpose. His or her phone records may have been accessed innocently or accidentally, or because he or she was incidentally involved in an investigation targeting somebody else, but nevertheless he or she should be notified of the fact that those records were accessed so that he or she can challenge them, if necessary, and say "No, my phone records were wrongfully accessed, I was put under surveillance for an improper purpose and I want to take this matter further". As Deputy Wallace has pointed out, at the moment Irish mobile phone companies appear to be unwilling to respect this right. At the moment, Irish law does not provide for this right. It seems to me that, because this is a requirement of the European Charter of Fundamental Rights, it is not just an obligation that is binding on the Irish State but an obligation that would be directly effective in the Irish courts. It seems to me that in an appropriate case, this would be binding on the Irish courts and indeed on the Data Protection Commissioner in assisting individuals to exercise their rights under the charter and under the GDPR.

Chairman: Deputy Chambers is the last member who has indicated.

Deputy Jack Chambers: Does Deputy Daly want to come in as well?

Deputy Clare Daly: I am after Deputy Chambers.

Deputy Jack Chambers: All right. Okay.

Chairman: Deputy Daly has just indicated. I want to make the point that we-----

Deputy Jack Chambers: I know we have someone else coming in.

Chairman: -----have exceeded the time we have been able to allocate. Our guest for the second session is here. I ask Deputies Chambers and Daly to be concise.

Deputy Jack Chambers: I thank the Chair. I thank Dr. McIntyre and Mr. McGarr for their presentations. I would like to comment on heads 58 and 91. There seems to have been a minimalist and anaemic approach to the transposition of Articles 56 and 82 into Irish law. How would the witnesses propose that the draft heads in question should be amended?

Mr. Simon McGarr: I would say the simplest and most effective way of dealing with the implementation of the GDPR would be to implement it using the wording of the regulation without an exemption in respect of the State's liability to compensation.

Dr. T.J. McIntyre: I am aware that Dr. Eoin O'Dell of Trinity College has produced a detailed piece on-----

Deputy Jack Chambers: Yes.

Dr. T.J. McIntyre: The Deputy has it. I would be in agreement with it. I would add a slightly technical but important point that he did not make. Head 91 deals with a judicial remedy which is not just damages but includes injunctive relief, for example in respect of the data subject. It does not have anything to say about the mandatory position under Article 81 of the directive that not-for-profit groups can bring actions on behalf of data subjects. In other words, it does not provide for a group such as Digital Rights Ireland to be able to bring a claim on behalf of an individual who has mandated it to bring an action on his or her behalf. I think the minimum that needs to be done is for the draft Bill to be modified to reflect that requirement.

Deputy Jack Chambers: I agree that the provision in respect of class action capacity should be transposed fully so that individuals are not undermined. Deputy Wallace mentioned State agencies. The Bill as drafted provides for such bodies to have less accountability than private organisations.

I would like to make a point about future health care technologies and data management. Many US states are trying to provide red-flag markers and prophylactic capacity with health care technology. Obviously, there is a need for significant and comprehensive data management and retention. I assume Ireland will move towards a health care management system that manages its health care population with better skills and has better outcomes for individuals. How will that fit into this? How will the State manage future health care data-processing systems that look at managing the population in a way that uses data control in primary care and in the hospital system? At the moment, we have a haphazard kind of mixed data-processing system, depending on where one goes. It is all spread differently across the health care system. As we move to a more centralised data processing system, as has happened in the US where there is a red flag capacity, how do we manage that and its benefits with the potential for individual data breaches? How does this Bill fit into that in the context of health care?

Dr. T.J. McIntyre: That might be quite a challenging question to answer in the time available to us.

Mr. Simon McGarr: Without pretending to be an expert on health care, I believe that the US system is a different system that does not have the same data protection rights that the EU has embedded in its Charter of Fundamental Rights. If the State wishes, which it should, to take advantage of the growth of new technology in respect of improving health care outcomes for people, it must do so by respecting those rights and by starting from the basis that those rights are the bedrock on which to build people's trust and deliver a lasting and reliable health care service. Unless that lasting and reliable health care service has the trust of the population, it will fail, as we have seen in other countries both within and outside of the EU.

Deputy Jack Chambers: It is a matter of data control. On one level we are trying to provide for the proper right to health care and a wrap-around for everyone at all levels. In terms of population health, the best way to manage each engagement with the health service is to record it. The health care systems in the US now provide red flag capacity, which means that they can look at a spread of blood tests and trigger a red flag within the health care system in order that someone can get an intervention before an acute event has occurred. We have none of that in the Irish context, but health care technology can do that now. We are balancing the potential to give greater health care rights to people against their rights to data control. It is just an interesting comparator of how we manage that.

Mr. Simon McGarr: I am conscious of the committee's time.

Chairman: The final contributor in this session is Deputy Clare Daly.

Deputy Clare Daly: I will be brief. I am very sorry that I missed the start of the meeting. I could not get out of an engagement. I believe the witnesses have made a really compelling case for why we as a committee should move away from the sort of patchwork quilt approach that is being taken to this legislation at the moment. I was struck by the comment that any law we devise should be accessible to the public. In its present form, the way in which this massive project is being structured is kind of beyond accessibility. In that sense, we have to take serious note.

I was struck by Mr. McGarr's comment about the Executive reluctance to absorb recommendations of the EU. He is very polite. That is an incredibly beautiful way of saying that we are on a collision course and are out of kilter with the rest of Europe on some of these issues. One hand of the State is potentially doing one thing around the health indicators and so on, meanwhile regulation and rights are going in the other direction. We have to do something. It could be possible to deal with how that collision is to be addressed in this legislation to an extent. I do not really have a question but just wish to say that. Without putting the witness on the spot or in a collision with the executive types, he is saying we need to reorder the way we have approached this. We need to look at the repeal of the present Acts and then perhaps write this GDPR as a form of full document with a domestic, Irish consideration. That would be far simpler, along with some other stand-alone regulation. I think it would be a much cleaner approach. Is that in essence what the witness is saying?

Mr. Simon McGarr: It is.

Dr. T.J. McIntyre: I will make one point on that. Some of the confusion that will stem from the structure of this is due to the fact that the GDPR is an independent instrument. The national

variations and flexibilities as regards aspects of the GDPR mean that people are necessarily looking to two texts. As a practical matter rather than a legislative matter, it would be very helpful were the Office of the Data Protection Commissioner or the Department of Justice and Equality to publish, after this process is over, a consolidated document that would include the text of the GDPR and, after each article of the GDPR, the relevant provisions of Irish law that give effect to, derogate from or take advantage of the flexibility of each aspect.

Deputy Clare Daly: That is a very strong point and one we have to look at further.

Chairman: Well noted.

I thank all of the members for their attendance and contributions. I thank Dr. McIntyre and Mr. McGarr for their contributions this morning and their very informative exchange with the members. As the committee knows, we will move on to Dr. Geoffrey Shannon in our second session. He has joined us in the Visitors Gallery and is very welcome. I thank both witnesses and wish them the very best.

Sitting suspended at 10.15 p.m. and resumed at 10.16 p.m.

Chairman: We are resumed in public session. On behalf of the committee, I welcome Dr. Geoffrey Shannon, special rapporteur on child protection, to address the issue of the Data Protection Bill 2017. Dr. Shannon is our final witness in this series of hearings and is very welcome. On behalf of the committee, I thank him for his attendance and for the submission of his very detailed pre-notice document, which has been circulated to all the members. The witness will be invited to make a brief address and that will be followed by an exchange of questions and answers with the members.

Before we begin, I must draw the witness's attention to the situation around privilege. I think he is familiar with the procedure. Witnesses are protected by absolute privilege in respect of their evidence to the committee. If witnesses are directed by the committee to cease giving evidence on a particular matter and they continue to do so, they are entitled thereafter only to a qualified privilege in respect of their evidence. Witnesses are directed that only evidence connected with the subject matter of these proceedings is to be given and are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, or persons or entity by name or in such a way as to make him, her or it identifiable.

I invite Dr. Shannon to make his opening statement.

Dr. Geoffrey Shannon: I take this opportunity to thank the committee for the invitation to address it on the general scheme of the Data Protection Bill 2017. I had the opportunity of listening to the commentary of Mr. McGarr and Dr. McIntyre and I share many of the views articulated on the general points. I am not going to dwell on the detail of the regulation. I am going to focus specifically on the children's rights issues, which I believe are quite significant and profound, many of which have gone unnoticed, yet will have profound implications for children, particularly on the age of digital consent. Much of what I will say today involves a much broader consultation on the issues that arise under the general scheme.

As we know, the general scheme of the Data Protection Bill is a crucial step in Ireland's preparation for the implementation of new EU data protection obligations and it provides a much needed update of existing data protection legislation in this jurisdiction, namely, the Data Protection Acts 1988 and 2003.

The two key items of European legislation reflected in the general scheme are the EU general data protection regulation and the directive on the use of personal data by criminal enforcement authorities. The general data protection regulation was agreed in 2016 and mandates higher data protection standards for data subjects, imposing increased obligations on data controllers and processors. It focuses on reinforcing individual's rights, ensuring stronger enforcement of data protection rules and streamlining international transfers of personal data. A point made in the last session is one with which I agree. As a regulation, the GDPR will take effect in this jurisdiction automatically from 25 May 2018 and does not require a transposition. Nevertheless, the 2017 Bill significantly gives effect to its provisions and provides derogations where permitted. I have identified at the outset of my presentation, for the ease of the committee, five key issues that are central to our consideration. The first is on the age of digital consent, which I believe should be set at 13 years of age. The Bill in its current form is silent on this issue. The second issue is on the need for a definition of preventative and counselling services in order that blanket blocking of sites does not prevent access to much needed, and increasingly online, services for young people. The third key issue is the right to be forgotten. I have strongly articulated for this right on behalf of young people. We all know that young people sometimes insert material online that they would regret afterwards. We need to recognise and acknowledge the vulnerability of young people. They need to have the right of erasure and this right is not mentioned in the Bill in its current form. The fourth key issue is the link between data protection rights and digital safety. I have spent many of my reports highlighting the importance of digital safety. Digital safety is not about creating a nanny state; it is about empowering young people to understand the benefits and downsides of the online world, especially in terms of young people's exposure to cyberbullying. There is another important and profound question in respect of adult data literacy. Much more needs to be done in this jurisdiction. I say this as a person who still has a Nokia phone, which means I am hugely challenged myself in the context of the online world. The fifth key issue relates to the processing of sensitive data. We have seen so much public discussion over the last year on the importance of ensuring that organisations that hold sensitive data protect those data and that sufficient safeguards exist to ensure that citizens' fundamental rights are not breached in circumstances where data end up in the public domain. This is at the very core of the general data protection regulation.

In addition, it would be interesting to know whether children have been canvassed in respect of this Bill, and how they perceive its current form. It must be remembered that children, like adults, have data protection rights under both EU laws and the existing Irish data protection regime. Children may not, however, depending on their age and level of maturity and understanding, be in a position independently to exercise these rights. In this vein, and throughout my presentation, it is necessary to bear in mind recital 38 of the GDPR. I am constrained by time and will not read the provisions but just wish to highlight them. I am very happy to engage in any discussion on the various provisions in the international instruments. This recital states, "Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child." It continues by stating, "The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child." I am particularly concerned about that and the absence of any definition in the regulation on what amounts to "preventive or counselling services". Recital 38 explicitly recognises children as a separate and particularly vulnerable group in society with regard to data protection issues and I believe that that must inform the approach taken in the 2017 Bill in respect of the protection of the personal data of children.

I shall now turn to the digital age of consent, which is a key children's rights issue addressed in the Bill. Part 3 of the general scheme of the Data Protection Bill 2017 sets out the heads of the Bill required to give further effect to the GDPR. Head 16 of the Bill is particularly relevant from a child protection perspective. It concerns the child's consent with regard to information society services and relates to Article 8 of the general data protection regulation, which sets the age under which children require parental consent to sign up to digital services – known as the digital age of consent. Pursuant to Article 8, where a child is below the age of 16 years, data processing shall only be lawful to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states, however, have discretion to provide by law for a lower age, once that lower age is not below 13 years. When the age of consent is set, the data controller is obligated to make reasonable efforts to verify in respect of children below the age of consent that such consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. There is no definition of parental responsibility. It is a term alien to Irish law and it needs to be clarified. I shall discuss this aspect later on.

Article 5 of the UN Convention on the Rights of the Child, UNCRC, explicitly recognises that children have evolving capacities and that as they get older, they have a greater ability to take responsibility for decisions affecting their lives. The aim of the general data protection regulation, in setting a digital age of consent, is to protect young people from commercial online marketing providers, for instance social media and gaming platforms. The current situation whereby the same data practices are being used to target teenagers as those used to target adults is absolutely unacceptable and needs to be tackled.

In head 16 of the general scheme of the 2017 Bill, in its current form, the Irish digital age of consent has not yet been set out. It is silent in this regard. In the explanatory notes to the heads of the Bill, a consultation process on the appropriate age threshold is described as having been completed and it was indicated that the results of this consultation will be submitted to the Government for a decision in due course.

It appears, therefore, that no determination on this critical issue has been made by the legislature at this point in time. I believe that Ireland should take the opportunity now to designate the lowest permissible age - namely 13 - as the age of digital consent for this jurisdiction. This lower digital age of consent has also been recommended by children's organisations such as the Children's Rights Alliance. Ahead of this meeting with the committee I took the opportunity last week to discuss the issue with the Ombudsman for Children, who supports my view that the age of digital consent should be set at 13 years of age. A variety of competing children's rights and practical realities support the argument that the appropriate age, having regard to the permissible age range delineated by the GDPR, should be the lowest age possible.

Members will see in my written submission that I discuss the key rights which include the right to participate. The right of the child to participate and be heard in proceedings concerning him or her is a fundamental principle of international children's rights law and is enshrined by Article 12 of the UN Convention on the Rights of the Child and in Article 24 of the EU Charter of Fundamental Rights. We heard Dr. McIntyre make reference to the Charter of Fundamental Rights, an instrument that is binding on our courts. We should have particular regard to it. It talks about children having the right to such protection and care as is necessary for their well-being. They may express their views freely and we need to make sure that happens.

The importance of the voice of the child and the child's right to participate in all matters has been promoted recently in this jurisdiction when the Irish people voted in a referendum on chil-

dren's rights, which must mean something. We also see it reflected in the Children and Family Relationships Act 2015. The focus, however, has primarily been on private family law matters such as guardianship, access and custody. In my view it is equally relevant in the context of the drafting of new legislation. Ireland needs to do much more in terms of meaningful consultation with children where the legislation affects them. This is why I urge this. I am delighted that I now have the opportunity to present a children's rights perspective because all too often, apart from discrete children's rights issues, the Legislature does not take into account the impact the legislation will have on children. Legislation such as this will have a profound impact on children into the future.

In line with the national policy framework, the National Strategy on Children and Young People's Participation in Decision-Making, 2015-2020 was launched. It discusses the participation of young people. Its goal is to ensure that children and young people have a voice in their individual and collective everyday lives and it explicitly acknowledges that their voice in decision-making requires a cross-Government response, with initiatives and actions from all key Departments and agencies.

With the national strategy and the recommendation of the UN Committee on the Rights of the Child in mind, it is unclear whether children have been consulted on the issue of Ireland's proposed digital age of consent. While the explanatory note to head 16 describes a consultation process on the appropriate age threshold, which it declares as having already been completed, there is no comment in the explanatory note on what this consultation process entailed and, in particular, who it involved. In light of the child's right of participation, I believe that the views of, at the very least, a focus group of Irish children must first be garnered before any final decision is made on this question. Information services technology and digital media play an integral role in the lives of our young people, as exhibited in statistics that I have attached to my submission. Instead of reading them out, I will try to assist the committee by providing as much detail as possible on the likely impact of this legislation on children. The committee will see from the statistics how critical it is that children are given an opportunity to have their perspective heard in this legislation. Therefore, I recommend that a consultation process takes place to ascertain the views of a variety of age groups of children on the issue of digital consent.

Freedom of expression and freedom of assembly are very important. The right to freedom of expression is a human right that is not confined in its remit to adults. The UNCRC guarantees a child's enjoyment to freedom of expression in Article 13. Further related rights under the UNCRC include the right to access appropriate information, provided in Article 17, and the freedom to assemble peacefully. Such assembly may take place in the context of an online environment. We need to realise that the world has changed and that these basic human rights are as relevant in the online world as they are in the world to which we are accustomed. That needs to be acknowledged in our legislation. These rights are often exercised by children through their use of information and communications technology.

If members examine the statistics that I have furnished in my advance submission, they will see that so many children spend a great deal of time on the Internet on a daily basis we need to consider how their rights are protected and vindicated in the online world as much as they are in the offline world. We have been slow to catch up with technology in terms of child protection and children's basic human rights.

In a number of my previous rapporteur reports, I have highlighted the importance of the Internet for children's freedom of information. While there is a genuine need and, indeed, obligation to protect children from the dangers of the Internet, the State must ensure that it does not

unreasonably restrict children's civil and political rights, such as the right to freedom of information and expression. The Child Rights International Network, CRIN, identifies instances of Internet service providers being pressured by state authorities to institute blanket filters to block websites containing material that is argued to be unsuitable for those aged under 18 years even though some of the sites contain material that could be important for the well-being of many under 18s, such as material on sexual education, politics and support groups for alcohol dependency and suicide. Alcohol dependency is an issue that I have articulated in strong terms in the context of my recent audit report. Society has been reluctant to engage with the issue and the Government has been reluctant to take on vested interests. Now the time is right to deal with the issue and provide supports. Sometimes, those supports can exist online.

The blanket filters to which I referred are arguably contrary to Article 5 of the UNCRC, which deals with children's evolving capacities. Restricting Internet usage for children, for instance, by setting the digital age of consent at 16 years, should therefore be approached with caution and the varying rights at play must be borne in mind. The overarching consideration must be whether any such restriction is in the best interests of the child. This is mandated in Article 24 of the Charter of Fundamental Rights of the European Union, which provides that, in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. I believe passionately that, to prevent any infringement of the child's right to express himself or herself freely and to ensure children's access to online information, the digital age of consent should not be set at 18 years, but at 13 years, which would be preferable in order to prevent a dramatic reduction in the participation of young people in online services. This is an important point that the committee should take on board.

Due to time constraints, I will move to my next critical point, namely, the definition of preventive and counselling services. The rights of children to participate in matters concerning them, to be heard, to express themselves freely and to access information need to be exercised effectively by children. On a practical level, therefore, certain realities must be considered to ensure that children are capable of exercising these rights in the context of their online activity and use of digital services. A difficulty may arise in circumstances where the view of the child is not aligned to the view of his or her parents or guardians. For instance, children may wish to access online services relating to sexual health or education, explore LGBT issues or seek support if they are being bullied. Certain service providers in these areas regularly require and retain personal data from the young persons who access their services in order to improve and fine-tune the operation and content of same. Thus, children's personal data may be processed and retained.

These types of issue may be ones that the children involved, for a variety of reasons, may not be comfortable discussing with their parents or guardians. Children and young people often contact organisations or services in confidence and arguably should be allowed to continue to do so without having to obtain consent from their parent or parents. If the digital age of consent was to be set at 16 years, this would in all likelihood operate to prevent children from accessing these services, something that cannot be said to be in their best interests.

While recital 38 of the GDPR specifically provides that the special rules relating to the processing of children's personal data, namely, the requirement for parental consent, should not apply in the context of preventive or counselling services offered directly to a child, whether the variety of service providers envisaged in that context will come within the definition of "preventive or counselling services" is unclear and needs to be clarified. For this reason, I am

suggesting that consideration be given to defining "preventive or counselling services" in the broadest possible fashion so that children can avail of support when they need it. I urge the committee to consider this point.

It will be also necessary to provide clarification on whether organisations that provide online support services to children will have to verify the consent of the child's holder of parental responsibility before processing the child's data for not-for-profit use.

My next point is on the related issue of the holder of parental responsibility and what that means. It should be noted that head 16 of the general scheme does not contain any definition of the phrase "the holder of parental responsibility over the child". "Parental responsibility" is a term that is more common to the UK and is not defined in our legislation. This issue arose in the context of the children's rights referendum when we examined moving away from the terms "custody", "guardianship" and "access", but that has not happened. For this reason, the Bill may be problematic. Who is the "holder of parental responsibility"? The term should be defined and include any parent and guardian of the child, whether automatic or court appointed pursuant to the Guardianship of Infants Act 1964.

What we saw with the commencement of the Children and Family Relationships Act 2015 was a broad range of family types being taken in from the cold and enhanced rights for a large number of citizens. We saw the creation of temporary guardians, an expansion of testamentary guardians and rights for foster parents under section 6C of the 1964 Act, which means that foster parents or those who have been looking after a child for a period of one year when no other parent is willing or able to act can now have guardianship rights. Those substitute parents on a day-to-day basis should be entitled to provide consent. If they are handling the real parenting duties, they need to have commensurate rights. Applying a wide definition to the phrase "holder of parental responsibility" is preferable so as to allow for a broader category of persons who may be responsible for a child to be able to give the requisite consent for the child in question.

A further concern relates to the involvement of the "holder of parental responsibility", in that many parents or guardians of children have lower digital literacy skills compared to their children. Despite this, the GDPR places the responsibility to manage children's data protection on their parents and guardians where the child is under the digital age of consent. Greater awareness among parents and a more robust information campaign are required. The Department of Justice and Equality produced a good document, entitled "Data protection safeguards for children ('digital age of consent')", but we need to go one step further. This necessitates the development of appropriate, child-friendly material by the Data Protection Commission "which convey an understanding not only of the risks that may arise when personal information is supplied online but also the remedies that are available under data protection law".

I have championed and advocated the right to be forgotten year on year in my reports. We need to consider this matter, particularly in the context of children. In my ninth report, I discussed the right to be forgotten and its importance from the perspective of a child.

The right to be forgotten was held to exist in the seminal Google case in Spain. In that decision the Court of Justice of the European Union held that an EU citizen had a right to request commercial search firms such as Google to remove links to their personal information when requested to do so, provided that the information was no longer relevant, emphasising that an individual's right to privacy overrode the public interest in seeking access to information in certain circumstances. Article 17 of the general data protection regulation concerns the right to erasure, known as the right to be forgotten. There is no specific head in the general scheme

that gives effect to that article.

The right to be forgotten is not only important for adults, although the public narrative has focused on this dimension. It is probably even more important for children, as they are less likely than adults to be aware that information they post online may be available long term. They may not consider the consequences of posting something online which may last long beyond their childhood. While not stated in Article 17 of the general data protection regulation, it is suggested Ireland should take the opportunity to include specific provisions on this issue in the 2017 Data Protection Bill. At a practical level, we know that with increased vetting across the world searches are undertaken. If a child posts something online, it could turn up in a search and have profound consequences. If there is anything the committee should consider in protecting young people and their vulnerabilities, it is ensuring the right to erasure reflected in Article 17 of the general data protection regulation is explicitly provided for in the 2017 Bill. As I argued, the relevance for children of the right to be forgotten should be acknowledged. Children should be educated on the matter and it should be understood the age at which an individual posts information online should be considered to be a very important factor in decisions on whether to remove an individual's personal information from sites.

Another issue I have highlighted year on year is cyberbullying and cyberharassment. These are profound child protection issues. I argue that the Internet is the new child protection frontier. We need to ensure our children are properly protected online. Much more needs to be done in that regard. When we talk about protecting children's data, it is also about protecting children. The general data protection regulation and the general scheme of the 2017 Bill cannot be considered in a vacuum. There are risks associated with young people maintaining an online presence which cannot be ignored. In this vein, the introduction of the Criminal Law (Sexual Offences) Act 2017 is to be welcomed and applauded. The Act demonstrates Ireland's commitment to better protect its children from online predators and specifically recognises the dangers that come with technological advances by creating a wide range of new criminal offences dealing with child pornography and grooming, with a particular emphasis on the use of information and communications technology in such offences.

A further concern associated with children's Internet usage is the prevalence of cyberbullying and harassment. Each year when I have raised this issue, I have received a large volume of correspondence from parents saying they are delighted I have done so as their sons and daughters have been affected. The issue needs to be much more prominent on the political agenda. We must take the necessary steps to protect our children as the problem is widespread. One EU study indicated that 21% of children had been exposed to potentially harmful user-generated content such as hate, pro-anorexia and self-harm material. In order to ensure children are protected from cyberbullying in their online activities and that their personal data are not exploited, regard should be had to the recommendation of the UN Committee on the Rights of the Child that states should "develop effective safeguards for children against abuse without unduly restricting the full enjoyment of their rights". It is notable that Article 6(2) of the general data protection regulation enables member states to "maintain or introduce more specific provisions to adapt the application of the rules to ensure lawful and fair processing".

To further address the issues raised concerning cyberharassment and bullying, regard should be had to the recommendations I made in my tenth rapporteur report which is soon to be published. I also endorse the recommendations of the Law Reform Commission in its 2016 report on harmful communications and digital safety concerning take-down procedures. When content is put up online, there needs to be an effective mechanism to enable it to be taken down,

which would ensure the efficient removal of harmful digital communications online. The proposed office of the digital safety commissioner of Ireland would thereby oversee an effective and efficient take-down procedure in a timely manner, regulating a system of take-down orders for harmful cybercommunications made for both adults and children. Alongside the right to be forgotten, there must be a procedure for taking down in a timely fashion offensive material posted online. That is why I am strongly supportive of the recommendations of the Law Reform Commission. The proposal made by the commission regarding the establishment of a new statutory oversight system appears to be a practical and viable solution to the current gap in Irish law. I also recommend that consideration be given by the Government to chapter 3 of the commission's report to enable progress to be made in this regard and ensure steps will be taken to establish an office of the digital safety commissioner of Ireland. There needs to be some joined-up thinking between the two offices. In the light of the publication of the general scheme of the 2017 Data Protection Bill, the office of the digital safety commissioner of Ireland, if established, should be required to liaise with the Data Protection Commission operating pursuant to the 2017 Data Protection Bill. Co-operation between the two bodies would be essential in protecting children and their data.

The provision on the processing of special categories of data is very important. Article 9 of the general data protection regulation concerns the processing of special categories of personal data. I have a significant insight into this issue as I have spent the last two years conducting an audit of the exercise by An Garda Síochána of its emergency child protection powers which I am sure will interest the committee. I have looked at over 500,000 fields of PULSE data. It has provided me with a unique insight into the discrete aspect of child protection within the Garda. It is the largest audit worldwide of the exercise by a police force of its emergency child protection powers. It is rich in giving us an insight into how the child protection system operates. By and large, I have found that the Garda goes to great effort to deal with children sensitively in these circumstances. In respect of data protection, it is equally relevant. When sensitive personal data are gathered, we need sufficient safeguards to ensure they are treated appropriately. That is why Article 9 is important. The processing of special categories of personal data is permitted where it is necessary for the provision of health, social care or treatment or the management of health or social care systems and services, subject to suitable and specific measures being implemented to safeguard the fundamental rights and freedoms of data subjects. I am a big believer in ensuring citizens' fundamental rights are protected. We need to ensure that where there are derogations from the regulations, there are checks and balances. If somebody's sensitive personal data are being used for what are purported to be health reasons, there must be accountability, which must also be the case where there are breaches and data end up in the public domain.

In the general scheme of the 2017 Bill heads 17 and 18 concern the processing of special categories of personal data. Head 17 permits the making of regulations for the processing of sensitive data where "necessary for reasons of substantial interest", while head 18(1) particularly provides that these categories of sensitive data may be processed where necessary for, among other things, "the management of health and social care systems and services and for public interest reasons in the area of public health". It can be imagined that these exceptions to the prohibition of the processing of sensitive personal data will enable the Child and Family Agency to process such data in the carrying out of its statutory role. It will inevitably include sensitive data relating to children and young persons.

The 2017 Bill only allows this processing to take place on the condition that suitable and specific measures are adhered to in order to safeguard the fundamental rights and interests of

the data subject. As identified in the explanatory notes to Head 18, it is as of yet unclear as to the extent to which the "suitable and specific" measures referred to in Article 9 and included in the Bill are intended to be additional or complementary safeguards to those already placed upon data controllers elsewhere in the general data protection regulation or whether additional safeguards will be required.

I am passionately of the view that consideration should be given to the inclusion of additional safeguards, particularly where a child's sensitive personal data is engaged and is to be processed by an agency such as the Child and Family Agency. This should be explored having regard to Recital 38 of the general data protection regulation and the special protection required therein for the personal data of children.

I thank the members for taking time to listen to me this morning. I am happy to take questions.

Chairman: I thank Dr. Shannon. I wish to call Deputy Jack Chambers to comment because he was the first to raise his hand. Before doing so I notice that Deputy Clare Daly may have to leave.

Deputy Clare Daly: Before I go I must thank Dr. Shannon for his presentation and put on record that I support-----

Chairman: I would like to make a point before the Deputy leaves.

Deputy Clare Daly: All right.

Chairman: I have listened to what Dr. Shannon has said. I am a former spokesperson on health and children aged up to 14 years. Recently Dr. Shannon appeared before the Oireachtas Joint Committee on Children and Youth Affairs to discuss the audit that he has referenced. I have spoken to colleagues since and realise that the focus of that particular engagement was particularly and almost solely on the area of Tusla.

Dr. Shannon has conducted a significant body of work. In fact, he is probably the only non-member of An Garda Síochána who has had direct access to carry out an analysis of the workings of PULSE. It might be of interest to members to know that PULSE is an acronym that stands for Police Using Leading Systems Effectively. I shall let members think about that fact.

Dr. Shannon published his audit earlier this year. It was sent to this committee and to the Oireachtas Joint Committee on Children and Youth Affairs. That committee has addressed its section of the audit. I think that the area that Dr. Shannon has addressed regarding PULSE would be of particular interest to us. I suggest that we invite Dr. Shannon to address us on the matter when we resume in the autumn. Such a meeting might prove very informative in terms of the scheduling of our next engagement with the Garda Commissioner. Nobody has presented us with such an insight before. I want to ask a question before Deputy Daly leaves. Do members share my view? Yes.

Deputy Clare Daly: I agree with the Chairman's suggestion.

Chairman: After Deputy Jack Chambers comments I ask Dr. Shannon to indicate if he is willing to come back to us and address this particular area of work. I call Deputy Clare Daly.

Deputy Clare Daly: I support Dr. Shannon's call for the lowest digital age of consent to be 13 years and for the widest possible definition to be approved.

I am also interested in the following and perhaps Deputy Chambers will also mention it. It would be incredibly novel to have a focus group that includes children. I do not know how one could make it happen. I urge the committee to consider establishing such a group. Dr. Shannon has produced an incredibly comprehensive report. How can a focus group have meaningful engagement? The committee could return to the matter. It would be pioneering to be the first country to introduce a focus group because digital stuff is so important to kids.

Chairman: I noticed that Dr. Shannon during the course of his contribution talked about parents, in their various guises and in the widest sense, having lower digital literacy skills. I also noticed that Deputy Wallace looked at me. He probably thinks that I tick that box.

Deputy Clare Daly: Deputy Wallace is a pro.

Chairman: He is.

Deputy Clare Daly: It would be great if the committee considered establishing a focus group. I am interested in following up on the matter. I thank the Chairman for allowing me to comment and I apologise for having to leave.

Chairman: I thank Deputy Daly and call Deputy Chambers.

Deputy Jack Chambers: I thank Dr. Shannon for his thorough and excellent presentation. Deputy Jim O'Callaghan sends his apologies. He cannot attend here as he has a number of conflicting meetings. As one can see on the monitor, the Judicial Appointments Commission Bill is being debated in the Dáil. He cannot be in two places at the one time.

Dr. Shannon has mentioned a few areas that I would like to discuss. As Deputy Daly mentioned, the right to erasure is something that I support. Dr. Shannon has managed to highlight in his presentation some areas that have, heretofore, been ignored but are fundamental to children's right. Officials from the Department of Justice and Equality attended here a number of weeks ago. On that occasion we raised these matters with them. Unfortunately, they failed to respond or give a reasonable answer for ignoring the full transposition of some of the issues mentioned in the report. As Dr. Shannon has detailed about the right to erasure, as people are vetted and the online world grows it is fundamental that people can be forgotten, particularly children.

As Deputy Daly mentioned, it would be a novel idea to introduce a full and comprehensive consultation process that involved children. Perhaps Dr. Shannon can give details about other areas that he is involved in where such consultation takes place. A focus group would allow children to play an active role in making decisions about issues that will probably affect their future children. We should engage with children now.

We have all seen the predatory targeting of children by parts of the advertising industry such as the gambling and alcohol industries. Studies conducted in the United States show that children had more knowledge of Budweiser than about basic things one would expect them to know. I am not sure how to address the problem but I believe that we should address it in this Bill. The Oireachtas Joint Committee on Health is trying to bring in the Public Health (Alcohol) Bill and address some of the advertising restrictions. This committee can address the matter and the digital age of consent when discussing today's Bill.

I agree with the call for the lowest age of digital consent to be 13 years. It is another area of the Bill that has been ignored. It seems the tough questions and tough policy responses have

been completely ignored in terms of children's rights. We need a comprehensive response and for the Bill, as drafted, to be amended. Now is the time to make a positive change in order to protect children's rights in the future.

Dr. Shannon has comprehensively addressed all of the issues. I am sure many committee members will agree with me that we should amend the legislation thus enshrining children's rights properly in the context of data protection.

Dr. Geoffrey Shannon: I shall first reply to Deputy Daly's questions in her absence. She raised an important point about children being consulted. I am quite happy to set out how the initiative could be realised. There are two options available to the committee. First, it can request the Ombudsman for Children to assist with a consultation of a large group of children. The Office of the Ombudsman for Children is well positioned to undertake such a consultation process. The focus group cannot be tokenistic and must cover a large number of age ranges. We have pegged the age of digital consent at 13 years and it needs to happen.

I must confess to having a vested interest in the Children's Rights Alliance. I am the founding patron of the Children's Rights Alliance. The Children's Rights Alliance has conducted a similar exercise. The alliance was responsible for children's voices being heard in Geneva. Their voices were incredibly powerful because children can convey an unedited message, which is what this committee needs to hear. All too often children are ignored when it comes to issues that directly affect them. The impact these provisions will have on children should be central in this legislation.

Deputy Chambers mentioned the age of digital consent. It would be a cop-out not to make a decision about the age of digital consent. It is a hugely important issue for children. If we leave the age of digital consent at the age of 16 in the interest of political expediency then we will have failed children. Children are much more adept at technology than their parents and will use technology anyway. We should support them in a way that allows them to engage with technology in a responsible fashion.

The right to erasure is hugely important. We all end up posting stuff online that we probably regret afterwards. We do not take into account the vulnerability of children. There is stuff that a child would post online that he or she would never post at 18 years or well into adulthood. We should not lose the opportunity of enshrining definitively in a Bill dealing with data protection the right to erasure and to be forgotten, alongside the take-down procedure. The take-down procedure is hugely urgent. Consider the cases that have come before the courts. There is a lack of legislation. The law must keep pace with technology and it has not. The victims are children. We say we are concerned about children but that concern must be matched by the necessary services and legislation for children. That is my view.

With regard to alcohol and gambling, I commend Senator Black on the extraordinary work she is doing on this issue. I feel like a fellow traveller when it comes to raising this issue, because one encounters huge resistance. I found over the last month that there is always some issue or justification from the alcohol industry, but I am delighted to have the opportunity to appear before the committee. What is staggering about my report is that the common feature across the shattered lives of hundreds of children is persistent alcohol abuse. I urge members to read chapter 3 which documents appalling abuses of children because of our reluctance to engage properly when dealing with alcohol. It requires a cross-governmental approach and it must be led from the top. We must continue to highlight this issue. I have argued that it is one of the biggest challenges standing in the way of children having the best possible family life.

The failure on the part of society to address the alcohol problem properly leaves the child protection system dealing with insurmountable consequences. That is how serious it is.

I feel strongly about the issue because I have spent two years looking at large amounts of data. Visions of one case I looked at will always stay with me. It involved a mother in a fast food joint throwing her child in the air like a ball because of alcohol abuse. Such stories permeate the report. I have always argued that after the outrage there must be action. That action is the Public Health (Alcohol) Bill. There appears to be a delay in passing that legislation, and the longer we delay the longer we put on hold the opportunity to help children who live in abusive environments.

Deputy Jack Chambers: The alcohol control Bill is being blocked as well for some reason.

Dr. Geoffrey Shannon: There are many of the same problems. I have a cynical view on this. There are vested interests playing into the reluctance to introduce key legislative measures. The Government must demonstrate its leadership by ensuring that we put the rights of children first. It is no use having a referendum on the rights of children if we do not follow it through with positive action. The positive action means dealing with the gambling problem, which I believe is significant, and the alcohol problem, which I believe is a national crisis.

Chairman: I have no issue with Senator Black making a comment on this small divergence, but we are here to address the Data Protection Bill.

Senator Frances Black: I thank Dr. Shannon. He is a breath of fresh air at last. I will refer to the Public Health (Alcohol) Bill because Dr. Shannon referred to it, and I thank him for that. At last, I feel that somebody else is being a voice for children and families who have been impacted and devastated by alcohol and Ireland's unhealthy relationship with alcohol.

To refer back to the data protection legislation, we must highlight the way young people are targeted by certain industries such as the alcohol, gambling and sex industries. It is shocking. The subliminal messages being sent to children in this area are a huge concern. It is very worrying, particularly with regard to the mental health issue. I wish to highlight, in particular, the importance of the bullying that takes place and the vulnerability of young children to that. I utterly support what Dr. Shannon said today. There is no doubt that everything he said should be included in this legislation. However, part of me believes there should be separate legislation relating to children and data protection. It is a minefield when one thinks about it. What Dr. Shannon said today demonstrates that fact. There are so many different areas where children need 100% protection.

I support all aspects of what Dr. Shannon said. I hope we will be able to include all of his recommendations in the legislation. I certainly will support that. I appreciate Dr. Shannon's support on the alcohol issue in this country, because I feel very frustrated. We are aware of the issues with the lobbying, the power of the industry and what it is doing to block the legislation to protect its profits, without any consideration for families, children and those who have issues with alcohol. It is a public health issue and it must be addressed. Profits should not be put before public health. I hope that the Government and the Opposition will support that legislation but, unfortunately, that is not happening and it is being blocked. I thank Dr. Shannon and I look forward to working with him in the future. I hope we can connect in the work both of us do in being the voice for those who do not have a voice.

Dr. Geoffrey Shannon: The Senator raised the important issue of having a discrete section

in the Bill on children's rights. In advance of this meeting I spent a great deal of time reading through the Bill to try to distil issues pertinent to children and that would be helpful in terms of bundling the children's rights issues together so we do not lose sight of them. It is about the visibility of children's rights issues in the legislation and the Senator's suggestion is very good. It is worthy of consideration.

Deputy Mick Wallace: There is much food for thought. I agree with the points made by Dr. Shannon. Children live in a different world. I have a few children and I can barely turn on the computer while they can take it apart and put it back together again. Unless we listen to them we will not understand them. People who legislate very often are disconnected from those for whom they are legislating, and that is probably more stark than ever in the case of children. It is crucial that we start to listen to them.

Chairman: Thank you sincerely Dr. Shannon for your presentation today. It was comprehensive. The supportive associated document that was circulated to the members will be a valuable tool in the consideration of amendments on Second Stage and beyond in the process of the legislation. You are the last witness to come forward on this matter and it was fitting that there was such focus on children. With regard to your audit of the processes and procedures relating to An Garda Síochána's employment of section 12 of the Child Care Act 1991, would you be happy to return to address the committee on that? The members of the committee have indicated a willingness for that. We will go into private session shortly when we can discuss the schedule. Would you be willing to return and address that section of your audit?

Dr. Geoffrey Shannon: I would be happy to address the committee on all aspects of the audit. It is a great opportunity for me, having spent two years and thousands of hours of work on it. It would be a pity for this committee not to have some insight. It also provides me with an opportunity to answer any questions the committee might have.

I have had the audit internationally validated in Oxford University. This is the largest audit worldwide of the exercise by a police force of its child protection powers. In terms of policing in general, it provides insight. It would be a pleasure for me to come back and address the committee on the issues that arose in the context of the audit.

Chairman: I thank Dr. Shannon. We will take that affirmation on board and will address it in our private session to immediately follow.

On behalf of the committee, there only remains for me to thank Dr. Shannon for his engagement here today, his contribution prior to it and the exchange with the members in regard to the general scheme of the Data Protection Bill.

The committee will suspend for one minute before going into private session to deal with housekeeping matters. I appeal to members to be patient with me. I will not keep them long.

The joint committee suspended at 11.10 a.m., resumed in private session at 11.12 a.m. and adjourned at 11.40 a.m. until 9 a.m. on Wednesday, 12 July 2017.