ADDLESHAW GODDARD

TRANSCRIPTION

GENERAL COUNSEL UPDATE (SESSION 2)

DATA PROTECTION AND PRIVACY

Nathalie Moreno

Just getting started. While you wait please sign up to our Data & Privacy Newsletter by scanning the QR Code. We'll be starting any minute.

Good morning everyone. Welcome to the second GC Update for 2021 which is dedicated to data protection and privacy law. I am Dr Nathalie Moreno, I'm a partner in the Data Protection Team and I have the pleasure to be joined today by Helena Brown and David Engel, two of my colleagues. Helena Brown is the Head of our Data Protection Team and David Engel is the Head of our Information & Reputation Team. As regular attendees will know, our GC Update Seminars are usually a full day of sessions and networking in our offices. Of course this year we are delivering those sessions slightly differently by holding it as a series of webinars over the first four Tuesdays of March and last Tuesday the GC Update covered Contract Law Update and Smart Contracts. Today we will start with a popular session on data protection law delivered by Helena. She will discuss how international data transfer rules are being affected by the decision of the European Court of Justice in tranche 2 but also the new Brexit Trade Agreement and she'll give us a fresh look on the new draft Standard Contractual Clauses which were issued by the Commission last November.

We will then have David discussing all you need to know about the variety and complexity of the data litigation risks that companies increasingly face and what are the options and actions available to companies when such claims arise be it individual claims or connected actions and to close our session Helena will give us an update on the investigations conducted by the UK Information Commissioner on the ad-tech industry focusing in particular on the real time bidding practices and on the recent Information Commissioner investigation on the data broking sector.

All along the seminar please feel free to ask questions by using the functionality, I will be monitoring these and putting them to Helena or David throughout the session after their respective talks and of course at the end of the Webinar with our Q&A sessions. I also need to let you know that this Webinar is being recorded and you will be able to access the recording after the session.

So on this, I think it's time for me to hand over to Helena.

Helena Brown

Thank you Nathalie for that introduction and welcome everybody to our slightly different GC Update on Privacy. As Nathalie said the first slot I'm going to focus on for the next 10 minutes or so is International Data Transfers. We have chosen this first because I think this year with Brexit and with the Schrems II decision it has been one of the biggest areas of focus and one of the biggest areas of concern for our clients. So I'll start with a kind of overview of where we are if I could go to our first slide what would be great thank you.

I suppose the first thing to know on international transfers is there's lot of moving parts, there's different things to consider and especially for UK businesses there is also the Brexit angle as well as just generally the international angle. The two big headlines in 2020 were of course Schrems II and Brexit so that's where our timeline starts. Our timeline starts in July and we got the Court of Justice decision on Schrems II which invalidated the Privacy Shield. Now I know this is quite a mixed group today, the Privacy Shield

was the safe transfer mechanism for data between Europe and the US and this is of course all going back to the principle that's existed since the dawn of data protection law that you can't transfer personal data to a territory that doesn't offer adequate protection. So under the Privacy Shield the US did offer adequate protection for businesses that were signed up to the Privacy Shield Requirements. That was challenged by Max Schrems privacy activist and that challenge was upheld in July and what that meant really was that everybody relying on the Privacy Shield as a safe transfer mechanism could no longer rely on it as of that date.

The biggest alternative adequacy mechanism is of course I'm sure most of you will know in a legal role the Standard Contractual Clauses which have to be signed by a data exporter and a data importer and once they're signed they create effectively adequacy provided of course that they're complied with and read and monitored and kept up to date but what happens with the invalidation privacy shield is the role of the Standard Contractual Clauses shifted overnight really into data reporting not only for US transfers but actually because of the comments that were made by the Court of Justice which effectively said "yes you can still use Standard Contractual Clauses but there are a lot of caveats around how you use them, there's a lot of evaluation you have to do to evaluate the territory that you are sending data to". The concept of transfer impact assessments started to emerge and it became very clear following Schrems the SCCs on their own would not necessarily be enough, so more about that in a minute. I just want to give you some more perspective as things evolved over the year.

In August 2020 we saw Max Schrems who is the founder and leads the "None of Your Business" Privacy Activist Group then on the back of his successful claim lodged 101 transfer complaints. Now that was just a gimmick, it was 101 because he wanted pictures of Dalmatians on the campaign to raise the profile of it but the point is a very serious one, and that was that businesses who had continued to use, primarily again targeting Facebook and Google, but these products which transferred data from the EU to the US. Businesses who'd continued to use them got a complaint, effectively it was very random, it was across all sectors, all sizes and it was really just I think creating an example. These complaints were lodged against businesses in multiple data protection authorities across Europe, we don't have any pronouncements on any of those decisions yet but really just emphasising the point and important to note that those complaints were made about continuing reliance on the Privacy Shield before the terms were updated but also around reliance on the Standard Contractual Clauses so the Schrems position remains that the Standard Contractual Clauses cannot be a valid transfer mechanism because the US doesn't offer a safe level of protection, that's not necessarily law of course but that's the view of the Privacy Activist.

Then we had a bit of an impasse, we had a bit of time to mull over what the impact of Schrems II was, what we all actually had to do in practice and we got in November the EPPB issuing draft guidance on the Schrems II decision which contained a fixed date assessment which gave some structure to organisations around doing these transfer impact assessments and I think although the concepts are perhaps unwelcome, we'll look a little bit at that in a minute, the structure and the clear steer in detail to do with guidance I think was to some extent welcome, it allowed organisations to get a perspective on what they had to do.

We then had really almost in the same breath I think it was a week later, the Commission publishing new drafts about contractual clauses so if you go back to what I was saying originally the Privacy Shield is invalidated, Standard Contractual Clauses suddenly become more important, we're getting new Standard Contractual Clauses and the reason we've got new ones is not just about Schrems, we've been expecting new ones for a long time because the existing Standard Contractual Clauses we've been using are very out of date, they had quite a few gaps in them particularly didn't cover transfers from processors to processors or transfers from processors to controllers so it was definitely something that needed to be updated and perhaps not surprising that the draft update followed what [♦09.58 *tape 1*] and Schrems II so again more on that but that will just be landed into the mix, now if I look at this timeline in terms of emoji's you know it sort of moves from amber to red if you're running a key business doing Brexit planning because at this point we're into November, we have no deal, we have Press saying

there's really not much prospects of a deal so UK businesses are thinking "well wait a minute I'm not going to be adequate as of Brexit, as of 31 December which means that my suppliers in the EEA or my customers in the EEA are not going to want to transfer data to me without something in place" so we then have this huge push to get adequate mechanisms in place to deal with a no deal Brexit which essentially had hoped signing Standard Contractual Clauses between UK businesses and their EEA partners and a lot of that was done pre-Brexit but we then got a special Christmas present on the 24th December when [♦11.01 *tape 1*] exercises and saying that actually there was what was a… what was it about the treatment of the novation agreement and under that agreement there would be a not adequacy for the UK but a bridge to allow transfers to keep happening between the EEA and the UK and to be deemed effectively adequate for another period of six months and that lasts until the 30th June, so what that's done is kind of perpetuated the, well in a sense perpetuated that certainty but we'll talk about that in a minute.

In January we got the EDPB and EDPS joint opinion on the new Standard Contractual Clauses and in February and this is where the emoji goes back to being slightly happier, we got the draft UK adequacy decision from the Commission, very recently, so again more on that, but it was certainly a step in the right direction and UK I feel is not counting its chickens on that but I think there's a relative feeling of confidence certainly from those that we speak to at the DCRS and in the ICO but they will be finalised but the caveat is the ICO has said if there's no adequacy by the end of April UK businesses will once again need to look at what their transfer mechanisms are so if you weren't one of the organisations that scrambled to put in place Standard Contractual Clauses to prepare for a no deal you may well have to that if it looks like we're not going to get adequacy before this bridge period ends at the end of June. Of course anything could happen between now and then and unfortunately I can't.. my crystal ball only goes so far.

So if we move onto the next slide.

We are then into really, and this is really just for you to have a quick look at, this is the six steps that were covered in the EDPB guidance. One of the important points I think to note is if we move away from Brexit for a minute is just Schrems II impacts every international transfer you do now whether you're doing it from the UK or not or whether it involves Europe or not you will have to do a transfer impact assessment essentially. My favourite box in this is the sort of rather bland statement you know assess the impact of third country national law and practice on transfer, just get a legal opinion on the national law to see how invasive it is, to see how much surveillance there is and I think that's the one that's causing businesses most concern in the EDPB guidance and to be fair in the Court of Justice decision as well because you know the logical interpretation of this is you need to keep the local law of any territory you're exporting to under constant review and as an importer you need to keep it under constant review and report back to your controller so taking this to its logical conclusion is a really pretty extreme set of measures and you will see that embodied as well in the new draft Standard Contractual Clauses which are Schrems friendly.

So if we move onto the next slide.

We can see that these principles that we've got from Schrems and these principles that we got from Schrems and these principles that are in the EDPB guidance are in fact now embodied in new Standard Contractual Clauses which I should say are not yet final so what we are seeing in some contracts already bearing in mind that the EDPB guidance is some additional requirements are being put in there to be Schrems friendly to include things like you know requiring your suppliers to monitor the law in the jurisdiction and update you if it changes and keep far more detailed audit procedures and you know just really trying to protect and again you know clearly the practicality of some of these provisions that we're seeing out there in the market at the moment and also bearing in mind that when new standard contractual clauses come in if you've updated your contract with those provisions they might conflict with the new Standard Contractual Clauses so you need to think about that if you're doing that.

Other headlines from the draft Standard Contractual Clauses, I mean there's some good news in there. As I said we've got four new models so in the olden days under the existing ones we're still in the olden

days, we've got only controller to controller and controller to processor. Under the new model we've got processor to processor and processor to controller as well so it definitely closes that gap and anyone who's had to deal with that you know gap you'll know its concrete because you're having to get contracts signed by controllers when really it's a processor to processor transfer or you're having to invent a new clause which doesn't quite fit and doesn't quite have the adequacy so you know this is good news and I have seen some businesses using the new draft just as a way of plugging that gap that exists at the moment in the hope that the final version won't be too dissimilar.

There are some other pretty onerous things in there that shouldn't be entered into lightly and the other thing I would say about the new Standard Contractual Clauses if you're going to need them, if they're going to be relevant to you, if you're doing business with the EEA, is there is a sunrise period so you have one year from which your existing contracts will be fine if they incorporate the old Standard Contractual Clauses but any new contracts will need to incorporate them so you'll have a one year period to implement another contract remediation and you need to be prepared for that because they are more detailed than the previous ones. There's various other relevant points in here as well. Just a word as we move onto the next slide because obviously the draft Standard Contractual Clauses will apply only to EEA transfers, they're a new law, they're going to be post-Brexit new law so it won't apply to UK transfers and just going back for a minute to the UK, as I said we don't have adequacy yet, the bridging mechanism ends on the 30th June, we've got the draft adequacy decision it will go through what's called a comitology procedure but as I say if you got it really keep an eye on your back up plan and just a point to note as well, adequacy doesn't wipe the slate clean on GDPR compliance if you're a UK business using personal data of EEA citizens regularly, you will still need to think about authorised representatives if you don't have a presence in the EEA and if you do you need to think about your EU needs to provide their authority as well and that won't change when adequacy comes in.

If we move onto the next slide, if we just remember what we were saying about the Standard Contractual Clauses the new draft only applying to transfers from the EEA, if you're a UK business what does that mean?

It effectively means you'll need to run two, or be aware of two regimes if you're doing business with the EEA because you EEA suppliers and customers will want to use the new Standard Contractual Clauses and as a business yourself in the UK you will subject to the UK version of the Standard Contractual Clauses whatever that may be and of course we don't have that yet. What the ICO has said is that UK businesses can continue to use the existing standard contractual clauses, they were very clear to say that's not the new Standard Contractual Clauses or UK transfers internationally because the new Standard Contractual Clauses will never apply in the UK but the old ones do, so again another confusing rule there is until such time as we have new UK Standard Contractual Clauses you'll need to keep using the existing Standard Contractual Clauses for UK transfers which is deemed to be fine by the ICO. I expect in 2021 we will get new UK versions of Standard Contractual Clauses, we'll get new ICO guidance on this and what I would also say is in the hope that there's adequacy perhaps UK businesses won't need to enter into the new EEA Standard Contractual Clauses regularly but it's all in a bit of a state of flux I'm afraid, so building in flexibility to your contractual models is really the name of the game at the moment unfortunately. I wish I could make it simpler, I hope that's made it at least clear what the issues are and if we've got time I can take a couple of questions.

Nathalie Moreno

Thank you Helena.

Helena Brown

We'll have a question Nathalie and do the rest if we've got time at the end.

Nathalie Moreno

So we can see the Data Transfer Rules are going through choppy waters and no wonder we have many questions on this. So you mentioned that the new Standard Contractual Clauses have not yet been

approved, what would you suggest companies do until those new Standard Contractual Clauses are adopted?

Helena Brown

Yeah that's a question we get a lot. I mean I think if you need to rely on Standard Contractual Clauses I suppose the first question is do your mapping of your data transfers and work out do you need to rely on Standard Contractual Clauses, has Schrems II made you nervous about relationships that you maybe should have had Standard Contractual Clauses in place or you haven't for example and once you've got your list of "who do I need Standard Contractual Clauses in place with?" look at what's actually in place, you know many existing contracts will already have Standard Contractual Clauses in place and those will be fine to keep using and as I said there's this one year sunrise period so you can by all means keep using them. I think the challenge is, and if you're putting in place new contracts at the moment, new Standard Contractual Clauses are not yet final so again there's a next section which I'll come on to, but for just now you should just keep using the existing Standard Contractual Clauses. The exception where you might want to think about using the new ones is where there is a gap you know where you've got a processor to processor transfer or a processor to controller transfer and you need to be pragmatic about this, if you're under pressure for whatever reason and your business needs these decisions for all sorts of reasons, I have seen some taking a view that actually we need to get this fixed now so we're just going to put in place a processor to processor based on the new version and have provisions around making sure the parties update that when the time comes to update it but thinking it is better to have something in place than nothing. None of that is perfect. Until we get the new Standard Contractual Clauses in place and until we get the new UK ones we're not going to have a perfect mechanism for processor to processor and processor to controller transfers so it's really just about finding the right kind of pragmatic approach for you and being aware that unfortunately at some point there is going to be a contractual remediation process and anticipating that you're technically letting somebody having procedures in place for potentially deemed acceptance, deemed accession to their Standard Contractual Clauses, that's one thing in the draft that we've got with the document clause at the moment but it is a personal thing for all parties, it's not brilliant from a deemed accession point of view but we'll see where that lies I think that was one of the comments that EDPB and EDPS had made.

I should say if you want to know more about Standard Contractual Clauses I'm doing another Webinar as part of our usual data download series which happens every two weeks, I'm doing that at 12 o'clock with further detail.

Nathalie Moreno

Thanks Helena.

Helena Brown

If you've got the stomach for more.

Nathalie Moreno

Lots of food for thought. Let me now hand you over to David who will discuss the many shapes and sizes of data litigation risks.

David Engel

Thank you Nathalie. Good morning everybody. As Nathalie said I lead the Reputation and, more importantly for today's purposes, Information Protection Team here and if I can have a first look please Emma, we're going to look fairly rapidly at four topics. First from the perspective of defending incoming, let's call them, data claims and we'll see why that may be a bit of misnomer but let's call them that for shorthand.

We're spending quite a lot of our time now acting for and advising businesses who are receiving these claims for distress as its usually put from data subjects who say that their rights have been infringed. So first of all we'll have a look at those rights. We'll look at the individual data claims i.e. where they come

in one by one or perhaps in groups. Thirdly at collective data claims that is class actions and where we are there and finally we'll have a brief look at looking at DSARs and one or two pointers in order to make sure that the way the DSAR is handled best protects your position in the event that that results in litigation.

Can I have the next slide please Emma?

Now what rights have been infringed? So Nomenclature does matter here. Data protection is not the same as privacy. I'm aware that the terms are of course used interchangeably in common parlance but legally they are two different concepts and that is quite important from the point of view of defending these claims. So normally there are three causes of actions relied on by claimants in these kinds of cases. First of they normally rely on all three, we do occasionally see some that are just a data protection case but it's pretty unusual.

So first of all you do have data protection claims so that's a claim under the GDPR and/or the new Data Protection Act and essentially that is a claim for an infringement of the regulation or the statue, typically a failure to comply with one of the data protection principles such as for example the security principle or processing personal data fairly, lawfully and transparently.

Then you have privacy which is a different legal concept which has its roots in the European Convention of Human Rights, Article 8 of which protects a person's right to a private life including their home, correspondence and family life and that over the last 15 or 20 years has morphed into a new tort in English also called "Misuse of Private Information" and in order to get home on a claim for misuse of private information the first point to take us on is the misuse, i.e. there has to be a use of that private information by the person you are purporting to make a claim against. Secondly it has to be information for which you have a reasonable expectation of privacy and thirdly that reasonable expectation of privacy which is your Article 8 Human Right mustn't be outweighed by any other Human Right, typically the Article 10 right to Freedom of Expression i.e. that a third party has the right to use and perhaps publish that private information. Thirdly you have yet another legal concept, confidentiality. Now I know we all put on our letters "private & confidential" and my friends sometimes say that so typical of lawyers why do they say the same thing twice, isn't it just like saying "null and void"? Is it so you can charge your clients twice over they even say but of course privacy and confidentiality are two different legal concepts. To succeed in a claim for breach of confidence you either are essentially enforcing a contractual obligation of confidentiality, you might see that in an employment agreement for example, or your equitable right of confidence or perhaps more accurately the breach of the equitable duty of confidence which a person owes you because they've come into possession of confidential information. So the structure is completely different and the nature of the information can also be different because something to be confidential does have to have what the courts call "a quality of confidence about it" i.e. it doesn't have to be secret but it has to be pretty confidential. The same doesn't apply to privacy.

Now that is really the end of the law for this morning you'll be glad to hear but they're worth bearing in mind because they are fairly subtle distinctions but very important distinctions and when one is seeking to sue you or threatening to sue you it does sometimes seem to be lost on the claimant firms who tend to just procedure their template letter of claim where they haven't really thought about this and perhaps they don't even understand some of this. In the words of Chris Whitty "Emma could I have the next slide please".

So looking at individual claims what do these look like and what have we seen? Well sometimes they are pure one-off claims i.e. one person who is saying that they have a claim for example because they visited a website and tracking pixels have been used and this was a grievance breach of Data Protection law. Other times it's a kind of slew of claims so you might have 3 or 4 or 30 or 40 but they're all individual claims they're not actually a class action.

Now an important thing to bear in mind is that all these claims are governed by a specialist pre-action protocol, again this is a point that is sometimes lost on the claimant lawyers and it's a very useful took because that sets out, and you can look it up online, that sets out some very specific requirements that

have to be spelt out when a claim is being intimated and it gives plenty of ammunition to go back and ask certain questions or really essentially just say to the claimant "you need to explain what your case is".

What is the claimant entitled to? Well, damages in privacy and breach of confidence and we've looked very briefly at how those may arise but also damages under the GDPR. Now as the DPAs amongst you will probably only be too well aware, that is a vexed and thorny issue. What is not a vexed and thorny issue is that you don't have to prove financial loss of any description distress is enough but there has to be evidence of distress and now potentially depending on what the Supreme Court says in *Lloyd v Google* loss of control over the data is also sufficient even if there's no distress.

Next slide please Emma.

You will see on the next slide I've set out some of the other damages that can also be received this is all under GDPR, identity theft unsurprisingly, damage to reputation interestingly and was successfully done in a case called *Ivans*, loss of confidentiality, so there we see some of the overlap coming in between the different causes of action and then this very broad category "Any other significant economic or social disadvantage". Now the important point about all of this though is the triviality threshold so again claimants will assert "well I lost control of the data", well maybe they did for whatever reason but they don't have a claim unless it's a non-trivial loss of control. In any event the damages are normally very modest, we're really looking at sort of £250-£1,000. There have been higher awards than that but of the counterclaims we see coming in they're very modest assuming there's liability at all of course.

Now what's happening out there from a practical/commercial perspective is that there seems to be quite a lot of fairly low rent firms for some reason often based in the North West of England who are seeing data claims as their new meal ticket and new PPI. They seem to be operating a lot of a sort of "no win no fee" type basis so you know they're getting their cash out of whatever they agree with their client they get out of you as it were and so their priority in addition to doing their best for their client is also to recover their own costs.

Can we have the next slide please.

As I said the onus is on the claimant to make his or her case and that is a really powerful tactical weapon as a defending business that you have. They must comply with the pre-action protocol I mentioned and that applies also to litigants in person so not just the represented claimants and it certainly applies if they're suggesting proceedings in the High Court which weirdly a lot of them do and probably the reason for that is they reckon they're going to get more costs back if they go in the High Court but equally they have more cost exposure so it's a slightly double edged sword for claimants but that does enable you to put claimants to proof at a very early stage when you get that initial letter of claim about things such as the Particulars of Distress about why they say they get over the triviality threshold. It is a novel and complex area of law, apart from anything else there's very little case law on it. If the claim is being issued in the High Court as they all say it's going to be, then it must be issued in a specialist Queen's Bench list for media and communications claims, that's even if it's a pure data protection claim and also as I've said they're normally data protection and privacy and confidence and again they all have to be issued in that specialist list which has certain procedures and so forth. So essentially you've got lots of ammo to throw at these claims that come in where on the whole firms are just after the quick cheque and you can see why because given the very low quantum value of most of these claims, for any business looking at each claim individually, it's got to make sense just to write a cheque because you're very quickly going to be writing a cheque to your own lawyers for more and potentially a lot more than any cheque you'd be writing to one of these people and therefore the first option to think about is either very early settlement or maybe even an ex-gratia offer to all data subjects affected by the breach or other issue whatever it is assuming you don't have a big class there obviously, but you know if you're talking about people in the tens or perhaps even the low hundreds that's an option but be careful because what we have seen is a claim will come in or maybe one or two claims and particularly if they come from the same firm and essentially what they'll be doing there is testing the water, they'll be seeing whether the business reacts by writing them a cheque or by defending themselves and the risk of writing

a cheque is that you know once you've done that then 500 claims come through the door. I mean obviously that doesn't compel you to deal with the 500 in the same way but it's a risk. Even if you're defending it you can obviously make a pre-action Part 36 offer which does protect your position on costs in the event that proceedings are subsequently issued but doesn't sort out the costs that you have agreed to pay. If you make a Part 36 offer what you're doing is you're saying "here are your damages of £500 or whatever it is and I'm agreeing to pay your legal costs to date". What can then happen if you have a lengthy wrangle about what those costs are.

Another thing to think about is are the proceedings going to be in the High Court or the County Court, there are pros and cons to both of those, I've already mentioned one or the main one really which is recovery of costs. That will be driven really by the strength of your defence.

Emma can we move onto the next slide please.

So that's individual claims now the other risk area at the moment kind of waiting in the wings to some extent but its real and its certainly underway is class actions, collective claims and one of the risks of that is that they're funded, i.e. they're funded by commercial litigation funders. Now this generally only applies in the situation of a mass data breach because the economics don't work for funders unless they've got a potentially very big class. Now you won't see any of the counter firms I've mentioned acting for claimants in these kind of claims, here you have normally you know larger, more established commercial firms but they will be generally acting on a damages based agreement which is a contingency fee or maybe a hybrid one i.e. where they get a certain amount of their costs paid as they go along but basically they're contingent on recovering. Next slide please Emma.

There are a lot of economics floating around there and that is essentially why most of these have not really got anywhere so far. Now what do these look like? They come in various shapes and sizes. There is the group litigation order type claims so that is where you have a group of claimants, it could be a large number, and generally it will all relate to a single data breach because there must be common or related issues of fact or law and an example of that is the case that is being brought against British Airways arising out of their data breach a couple of years ago where 420,000 I think it was passengers or customers of British Airways had quite a lot of data stolen. Those claims are "opt in" in other words anybody who wants to join the claim has to sign up for it so that is to some extent a kind of known quantity and if we have time we can come back and maybe look at the pro's and con's from the claimant's perspective of those kind of actions.

Now the novel development really in this area, we've seen them in competition cases but certainly in the data and privacy area representative actions which are opt out i.e. if you were affected by the data breach, provided you can satisfy the same interest test i.e. you have the same interest in the claim and importantly suffered essentially the same damage, you are in it unless you opt out. I'm sure many of you will be familiar with the case currently going through the courts against Google headlined by a representative claimant Mr Lloyd who is represented by Mischon de Reya. Now that was in the High Court and the Judge Mr Justice Warby as he then was, was extremely dismissive of this as a means of getting compensation for data breaches and was rude about the lawyers and the funders and said you know "the only person who's going to make any money out of this is going to be the lawyers and the funders, no, no allowed". So the claimants went to the Court of Appeal, the Court of Appeal said "yeah it's all fine crack on" so Google then took it to the Supreme Court and that is being heard next month in the Supreme Court and we shall see what the upshot of that is and we probably won't know until possibly the back end of the Summer but more likely it will probably be Autumn.

Then you have informal collective procedures where you have maybe lots of individual claimants of the sort we looked at earlier and they sort of get together and maybe consolidate their claims.

Emma could I have the next slide please.

So if you're faced, which hopefully you won't be but a number of businesses have been already, with one of these collective class actions plainly there is, you're in a whole different ball park here in terms of potential financial exposure because although damages are modest per capita none of that changes

and obviously you have potentially a big multiplier a big class of people so in the *Lloyd v Google* case for example the claimants have already said we'll take 750 a head but there are about 4 million potential claimants so that is clearly a big number. Costs are going to be huge as well because these cases are not cheap to run as a claimant, as a claimant law firm and they're not cheap to defend either.

Now the Supreme Court decision in *Lloyd v Google* I mentioned earlier will definitely influence the future direction of travel. The two main issues the Supreme Court is going to look at is can you recover damages for loss of control on a uniform basis across the entire class so in that case does this £750, you know, is the court happy to accept that the damage essentially is going to be the same for every member of the class? Bearing in mind you know that some members of the class don't even know that they're in it, the *Google* case was about the Safari work around essentially that enabled Google to track internet usage but of that 4 million how many is anyone's guess won't even have been aware of it so you know should they be entitled to damages? An interesting philosophical question which we don't have time for today and a related point can an opt out class action of this kind meet the same interest test i.e. can you actually say that they all have the same interest in the litigation?

So watch this space. If the Supreme Court disagrees with the Court of Appeal and essentially says "we're not happy about this as a means for compensation" that will probably pretty much be the death now for these kinds of collective opt out actions.

Emma, next slide please and I think the last one and I'm really hoping I'm running to time.

Finally, a very quick word about DSARS, we're not here to talk about DSARS, I'm sure you've all heard more about DSARS than you could reasonably wish to. My point coming at it with my litigator hat on is a very simple one, be careful. Is it compliance or contentious work? In our experience people very rarely make DSARS, well sometimes they do but on the whole they've not taken out DSARS because they can't think of anything better to do with their time, they're doing it for a reason. Generally it's a precursor to litigation maybe a complaint to the Regulator, maybe they want to leak something to the Media or put it on Social Media or whatever. Now the *Taylor Wessing* case *Damer v Taylor Wessing* established that none of that is relevant, none of that impugns the validity of the request, you still have to reply with the request. So what we would say is act like a compliance officer, obviously you have to comply with your duties under the GDPR to answer the request but think like a litigator, err on the side of caution, don't give requestors material that you absolutely don't have to, think about the exemptions and apply them, think how much can be redacted, remember they're only entitled to their personal data, they're not entitled to documents. I know sometimes it's easier to provide a document but there may be good reasons why you don't want to see that document on the front page of the Mail on Sunday for example or on YouTube and ensure that your processes or the processes that you use are fit for purpose and that probably involves using some kind of AI platform to simplify, speed up and make less expensive the document review and redaction process and Helena wont forgive me if I don't very quickly mention that of course we have got an A1 AI system here and we help a lot of businesses with handling their details on that kind of basis. So unless Dr Moreno has any tricky questions for me or anyone else does that concludes my slides.

Nathalie Moreno

Thanks very much David and yes you're right we have tricky questions. We have many actually but I'm gong to spare you the Scottish question I'm going to go to a question which probably is relevant to everybody. Do you ever see claims for breach of GDPR alone or do they always come with a claim associated to privacy and breach of confidence?

David Engel

Yes, as I said we don't, I'm wracking my brain now but I'm pretty sure we haven't had any in and we've had a lot over the last 2-3 years that have just been put as breach of the GDPR, there may have been 1 or 2 but they're a very small minority. The one that sometimes drops out is breach of confidence sometimes that's not included but always a privacy claim is included and generally a breach of confidence claim as well. Its helpful because you know you may have defences, well it cuts both ways,

very often there is a defence to the data protection claim for example it was a one off data breach but actually the systems are all fine you know the technical and organisational measures are all fine, therefore no liability but there may still be liability for example in privacy, that happens quite a lot actually because the information has got into the wrong hands or whatever it is and it can cut the other way as well. Or you may have a situation where there is a technical breach of the GDPR but actually you're fine on privacy because no-one has actually used it or at least you know a business hasn't used that private information in a way which would constitute tortious misuse.

Nathalie Moreno

Okay thanks David I think that's pretty clear. Okay then I think I'm going to hand over to Helena for her next session on Ad-tech and Marketing.

Helena Brown

Thank you Nathalie, I'm just checking you can hear me okay. Yeah, I'm always conscious about unmuting myself. Okay this won't take long I just wanted to say about the other thing that has been causing a bit of change and a bit of concern is the movements around use of AI and ad-tech and also just consumer engagements and the investigation into the data broking industry.

So what's happened this year if we move onto our first slide here. The ICO as some of you might be aware in 2019 launched an investigation into ad-tech and real time bidding so that's the thing that seems to know when you want to buy toothpaste and you go on Amazon and you get adverts for toothpaste you know it's weird and that's the process by which you know somewhere along the lines we're being tracked, we're being monitored and particularly that ad space is being sold to the highest bidder.

The investigation was launched in 2019 and that was suspended due to Covid 19 in the May.

The next point on that list is the ICO obviously has been investigating the data broking industry since well its really since GDPR came into force, and that part of the investigation concluded in October this year. We had an enforcement notice, not a fine, but an enforcement notice against Experian which will be capped quickly. I should say that that is currently under appeal and I believe there's a hearing today on it so there will be more to come on that, there are some really interesting shifts here around some concepts, around the use of legitimate interests and consent around postal marketing but also very relevant to ad-tech.

The ICO re-opened their investigation in January into the ad-tech industry and real time bidding as well so they have now made a request to audit four of the platform traders in this space so that's going to be changing. You also need to bear in mind all of this activity is covered or much of the activity is covered by the Privacy & Electronic Communications Regulations 2003 which have not yet been updated although consent standards were updated under GDPR the basic requirements around tracking cookies, pixels and all these things are still set out in the 2003 Regs. There is a new EU Privacy Regulation trundling through the process of approval and they've got a further step forward on that since February, the counsel's opinion on that published which is really business friendly I think and preserves things like the soft opt in for businesses. Of course the question will be to what extent the UK implements that but that's for another seminar I think.

A significant development just in the Wall Street Journal reported last week that Google had announced a plan to stop any individual tracking by 2022 and that's really significant because that's about not supporting third party [♦20.08 – *tape 2 – interference on recording*] ad-tech industry so there's going to be some really significant changes there and I just wanted to highlight this because it feels like there is a storm brewing around this, I mean you just need to be aware of it when we're entering into new relationships and making new [♦20.29 – *tape 2*] for consumer engagement.

So if we can move on to the next slide. This just gives a little bit of a summary of the concerns really about as I said ad-tech and real time bidding, its invisible there are long complex supply chains for this data its really difficult to get Privacy Notices to people. Its really difficult to get the consent needed to attach those cookies and I'm sure most of you are probably not aware of giving consent to these things.

The ICO has been quite bold in its statement stating if you think non-compliance is likely because it is looking at the nature of these services it's very difficult to show transparency and demonstrate the consent that you obviously need to demonstrate and you would not have any findings yet I expect but that that will come.

If we move onto the next slide. Let's look at what we've got so far. I should say that I'm kind of jumping here between real time bidder and ad-tech online and the ICO's data broking investigation because actually these two things need to be read together. Although the ICO's data broking investigation started with postal marketing only so offline marketing only they will move on to online marketing and they have specifically said as part of this new launched investigation that they will be looking at the role of data brokers in their investigation into ad-tech so it's really relevant to see the direction of travel and aside from the relevance to ad-tech this investigation is also really relevant to anybody who is using these databases as a way of augmenting marketing databases. I'm very conscious of time so I'm not going to go through this in a huge amount of detail but you can see on the slide there that there is you know a really thorough investigation and it's a very expansive product that they were looking at, it's the Experian Consumer View and ChannelView products so covering I mean a huge number of adults in the UK, using information from public sources but also private suppliers with a bit of credit reference information into the mix there. Really the crux of the concern the ICO had is with the use of data by individuals in a way that's unexpected so even though it wasn't online, it wasn't about using cookies or tracking behaviours online or listening to people, it was about using publicly available information to make some perhaps unexpected decisions about people and that was enough for this enforcement notice to happen.

So if we move onto the next slide we can see this is a summary of what the breaches are and anyone who is really interested in this area I would urge you to read the enforcement and read the Experian response because on the one hand we've got Experian who have actually an incredibly detailed privacy notice which was updated throughout the course of the investigation in an attempt to you know avoid an enforcement which ultimately wasn't enough, but if you look at it it's incredibly detailed but you know these principles are relevant to all of us and I think it just shows the direction of travel with the ICO on this.

So we've got fairness and transparency breaches you know the logic of the AI wasn't provided, wasn't explained so what are they actually doing? How are these decisions reached? What factors are they considering to decide if your wealthy or you're likely to buy a product or whatever you know the characteristic is that they're trying to sell as one of their segments or mosaic. Also the language you know looking at the criticism of the vague sort of marketing speak that's used, so a very practical thing you can take away from this right now is look at your privacy notices, do you explain how your using automated decision making, do you explain the logic behind it, are you using clear language?

The next pillar legitimate interests breach is super interesting because it actually challenges the legitimate interest assessments that we've all been doing. Now it's very clear from GDPR that legitimate interest is a legal basis that can be used for marketing but what the ICO was saying in this enforcement is because of the volume of profiling and the fact it was very unexpected and because you know there was what we call "significant intrusion" making decisions about wealth and things like that it resulted in an imbalance such that legitimate interests shouldn't be used. Even if you can argue that nobody is particularly distressed by marketing it shows a changing of the dial on legitimate interests interpretations and this is of a bit of concern and I certainly see that behind the scenes in our practice as well and in approaches that the ICO has been taking to some investigations which don't ever hit publication like this one has, but it's certainly something you need to be aware of if you're doing LI's and bear that in mind. I'm not saying Legitimate Interests can't be used for marketing of course they can and I think it should but you must bear in mind that this has been appealed and may well be, some of these findings might be reversed and the other point here was the Consent Breach which is perhaps not surprising but some of the suppliers couldn't demonstrate that they had actually obtained appropriate consents. I mean I think most people are wise to that that if you're relying on consent you need to be able to demonstrate

it and the problem with this is of course that Experian and logically its customers who are using these sets of information are actually not relying on consent, they're relying on Legitimate Interests so if the initial supply of data has relied on consent the ICO is saying you can't then switch to Legitimate Interests.

So there's lots of food for thought in all of this and you know again it's a really moving piece so I'm not saying switch off everything that you're using you know I think Experian are pushing back pretty strongly on this and use some might argue for good reason because of the extent of the interpretation of Legitimate Interests.

If we move onto the next slide. What can you do practically? On the ad-tech side of things this investigation is ongoing. It is likely that there will be findings and ultimately perhaps enforcements if the practices don't change so just think about that if you're using ad-tech. I know it's an incredibly efficient way of reaching consumer audiences and marketing teams are keen to use it so to protect yourself at the moment have a look at the guidance the ICO has on it right now, have a look at the DNA guidance, look at your supply chains, look at your contracts, can you protect yourself and crucially can you get out of them if things turn sour really in this kind of area? Also just remember that this is going to change even more significantly in the longer term when Google switches off its support for third party cookies and ultimately you know Experian will wait and see what happens on appeal but right now just consider your sources, are your notices clear and do everything you can to protect yourself.

I'm very conscious of time so I'm going to hand back over to Nathalie to see if we do have time for any questions.

Nathalie Moreno

Thank you Helena. We have so many questions that I'm just going to pick one in particular. One for your Helena and another for David. So Helena you've just mentioned about the Experian enforcement, does it mean that now companies do all over again their Legitimate Interests assessment on marketing?

Helena Brown

No, not at the moment. I think by and large Legitimate Interests for any marketing will in principle be possible if the balancing test turns out the right way around. I think what it does do is it might change your conclusions so if you've had a borderline LIA where you've maybe thought "hmm I'm not sure about this will people really expect to get this from us?" in light of the Experian enforcement you should be thinking twice about concluding it's okay, so I would say for the borderline ones I maybe would look at them again but the point is that there is plenty else to be doing for data protection teams and in-house legal teams at the moment there's all this stuff going on with the Standard Contractual Clauses, so I would probably advise you would think about it for new projects, keep an eye on the movement, sign up to the Privacy Bulletin and you'll get updates on this and will see how things change when this is appealed if they change or if they solidify in which case you need to at some point look at redoing LIA's but for now I probably would just bide your time and just bear it all in mind and keep track of the developments because it's pretty fast moving.

Nathalie Moreno

Thank you very much Helena and one very quick one for David. Does the pre-action protocol that you mentioned apply in Scotland?

David Engel

No. That's a very easy answer. No litigation procedure is completely different in Scotland. I am not qualified in Scots law but we have a team in Edinburgh and Glasgow which certainly is so if anyone would like me to put them in touch with one of them I can certainly do that but it doesn't apply nor I should say my understanding, I think that's the approved insurer's caveat, my understanding of the Scots procedure is that there isn't an equivalent either.

Nathalie Moreno

Understood. Thank you so much both of you for a fascinating discussion. I just want to mention one word about our next GC Update which will cover Employment Law and will take place on the 16th March. Thank you very much to our audience for their attention.