Regulating the GDPR: Perspectives from the United Kingdom

*Hannah McCausland**

Leila Javanshir: On behalf of the law school, the *Law Review*, and our CLE department who has partnered with the *Law Review* this year to make this CLE possible, we want to thank you all for attending our program today. We have an incredible lineup of speakers that are really looking forward to today's discussion on the topics we have set out. I wanted to provide a little bit of background with regard to the symposium itself. Every year, *Law Review* hosts its annual symposium on a topic that we feel demands attention and guidance, and then we invite our experts to not only come speak at the symposium, but also to write articles that we will then publish in our spring issue.

I know many of you have been dealing with the GDPR for the last year, probably the last two years for many of you, so we hope that today will act as a check-in as to where we are eight months after the regulation's implementation. As I noted already, we have an amazing panel of speakers throughout the day. They come from a wide array of professional backgrounds: we have individuals from the regulatory and enforcement side, the policy reform side, we have in-house counsel that deal with start-ups and the advancement of our artificial intelligence, we have some of the lawyers from the bigger firms in Seattle specializing in privacy and data security. We are also fortunate to have with us a couple data security compliance experts and some of the top academics that deal with this area of law.

Our speakers should be able to provide significant value in that they can cover all of our GDPR related bases, so we hope that you will take advantage of this opportunity and put your questions forward. Don't be shy because they really are here to provide guidance. I've had the pleasure of working with them over the past few months and they are eager to answer your questions. Lastly, at the end of the symposium we will be

* The author is Group Manager for International Engagement at the UK Information Commissioner's Office. This draws from experience gathered by the author over the last nine years during the development of the GDPR in Brussels and subsequently adopted into UK law.

holding a reception just two floors up. There will be food and drinks, so we hope that you will be able to stick around and chat with your colleagues and our experts. Without further ado, we can go ahead and get started. I'm going to introduce to you Professor Steve Tapia, our moderator for today's program. He has been practicing in entertainment media and intellectual property law for over thirty years. He is also a professor here at Seattle University School of Law. Thank you.

Steve Tapia: Welcome. Dean Clark sends her regrets. She is under the weather this morning, literally and figuratively, and couldn't be here. So, on behalf of her, I welcome you to Seattle University Law School. For those of you that are students or alumni, you know what we're doing here. For those of you that are visitors, let me try to give you just a couple seconds about some things that have happened over the last four or five years that have made Seattle University a little bit different than the Seattle Law School that you knew.

Over the last four or five years, we've really tried to put an emphasis on being nimble in a world that is changing very quickly. We have really put an emphasis on trying to create an interesting set of programs around innovation, technology, ethics, and privacy—with an immersion program, which was our first major effort which is a week-long deep dive into what it's like to be in-house counsel, having to deal with ethics, and technology issues and intellectual property issues in a world that's changing so fast, that a lot of times business people's best goal is to try to see if they can end-run legal as often as possible.

We have really created a set of programming that is really keeping our students interested. There are a lot of you that have been in my class—I recognize the faces—that can testify to the fact that we're at least making the effort to really try to equip the lawyers for the twenty-first century that Seattle has told us that they need. Being smart on privacy is certainly one of the key issues and that's one of the reasons why we're spearheading this effort.

I have to thank the *Law Review*; they've done an amazing job. Not just in supporting this symposium, but in generally steering what is traditionally a social justice-oriented agenda towards some really interesting innovation and technology topics, and devoting an entire issue to privacy is a testament to how the *Law Review* is actually, along with the faculty and the staff and the administration, really trying to move this school into areas that are new, challenging, and serve the world well. So, for those of you that are strangers to Seattle University Law School, I hope you come and visit us for some of the other things that we do. For those of you that are here now, thank you for being here now and being interested in these topics. For those of you that have gone through before, we deeply,

deeply appreciate your support, and it's really wonderful to see you in the audience here today.

Okay. I'm going to introduce Hannah in a second, but one of the things that I want to advise you is, because of the fact that we're using video technology here, Hannah can't see you or hear you, so if you have questions for her, there are notecards that are either being passed around or have been passed around. Please write down your questions. The student helpers will be around to try to collect them for you, and I will be asking her the questions at the appropriate moment. Because of the technology, we're going to try to let Hannah get through her presentation first and then we'll have a question period at the end.

That being said, let me introduce Hannah. Hannah McCausland leads the international group at the UK Information Commissioner's Office (ICO). The ICO's International Engagement functions as the gateway to other data protection and privacy authorities on international matters. She's involved in the work of the EU European Data Protection Board advising the commissioner and the deputy commissioner on international positioning of the ICO, and she has played a key role over the past six years in the ICO's strategy on navigating the EU's data protection framework. Hannah has also played a major role at the global level and advancing the practical tools that data protection and privacy regulators can use for enforcement cooperation. Prior to the ICO, Hannah worked both in Brussels and Amsterdam for almost ten years on international data protection regulation. In media and research sectors, she holds degrees from the London School of Economics and Political Science, and I can't think of a better person to kick off this symposium on European data privacy issues than Hannah McCausland.

Hannah McCausland: Well thank you so much, Professor, for the very kind introduction. Many thanks to Rebecca, Leila, the team, and everybody there at the University of Seattle. It's really a pleasure to be there with you today, albeit virtually. Well, there's plenty to get through today. I also look forward to receiving your questions at the end of this as well, but the way in which this is evolving, we're in a very highly changing, exciting regulatory landscape at the global level and I've had the privilege to be able to see the changes from the global view over the last few years. They say a week's a long time in politics, well, imagine more than six years so far on GDPR. I've been working on GDPR development in various guises, in different countries since around 2010. The way in which we're looking at GDPR now is really, really interesting because we've got a lot more responsibility as regulators, and we have a lot more expectation from the individuals, or data subjects as we know them here in the UK. There's a lot more expectation placed on us. To give

a bit of a context, I'm very much aware that in the US this GDPR came as a bit of a shock to the system on the twenty-fifth of May last year.

When you look at the press headlines, you see that influential entities were quoted in the media. For example, Russell Group with Risk Management Software Company, said that "GDPR could blow the lid off global digitally connected trade," and all of the newspapers and press in the media group, Chalk Ink, such as well-known titles like *L.A. Times*, *Chicago Tribune*, *New York Daily News*, were blocking EU users from using their websites, blaming GDPR. So, there were all kinds of fears about balkanizing the internet and creating a two-tier system of internet, and I'm going to look at a little bit at how those claims were probably for a bit of media hype and rather unfounded.

So, how we'll cover some of the key areas today, is that I'll give you a general overview: first, into items of our ICO experience of GDPR so far; then we will be looking a bit at the ICO's Regulatory Action Policy, how that has evolved since GDPR; next, looking at the new ICO horizons, what kind of new roles have we been taking on, what kind of new departments that we have been creating, and what new set-up; I wouldn't be surprised if I get questions about this afterwards as well, but I'll take a look with you at the expanded territorial scope of the GDPR; we'll take a look at the role of the new European Data Protection Board; and finally, a quick round to the EU–US Privacy Shield.

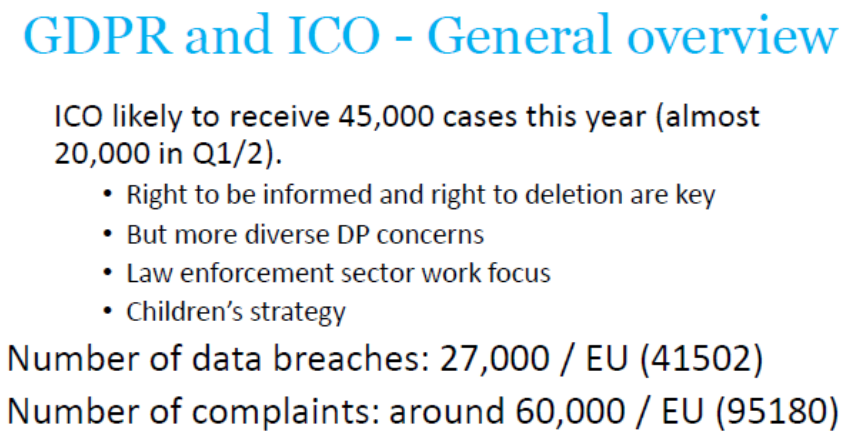
So overall, we've got ICO as one of the supervisory authorities in one of the twenty-eight EU member states. We are a member of the European Data Protection Board. We go to meet our European counterparts at least once a month now, that's far increased contact compared to pre-GDPR times, and our independence from our respective governments that we uphold is of utmost importance to all of us around that table.

The way in which we have evolved means that we've got many new feathers added to our hat, our regulatory hat, and we have far more regulatory teeth as well. So, we need that to meet the far higher expectations that individuals now have of us. In terms of the way in which we have been able to cope with our new role, we've had to move fast, and we've had to actually grow pretty quick as well to meet the demands posed by the volumes that we're facing. So, we've got approximately 95% increase in data protection receipts and the initial spike took place across all sectors, both in business and public sector for data breach notifications as well.

So, in quarter one of GDPR era, so after May 2018, the demand was extremely heavy for the ICO. We do expect this trend to continue, and I think we were notified just in case and we did expect that to continue;

however, that initial spike did level off, and we've seen a calmer data protection and business community now. Now we have the experience of about seven months, eight months under our belts. In terms of what we have been able to do within the ICO, we're actually able to respond to complaints within twelve weeks for 90% of that volume. So, we redeployed resources across the organization from all different departments to focus on the handling of complaints to make sure that we can handle those new volumes and uphold those individuals' rights.

In total, we're probably likely to receive in the region of 45,000 complaints or cases this year. I say complaints or cases because indeed we will receive cases which are not complaint-based necessarily. Sometimes you might get something referred when we spot it in the media or through another investigation that we're doing into a particular sector. But the way in which GDPR has affected our work means that we take a far broader view of the impact that data processing is having on individuals. So, whereas under the old data protection regime, before the twenty-fifth of May, we would have been focusing quite heavily on security breaches, now we're looking at far greater range of rights which individuals are concerned about, whether that's the right to be informed, the right to deletion or otherwise known as the right to be forgotten, in terms of searching the listings. There's a great focus that we're now taking, that we've identified needs our focus in the law enforcement sector, and we're also looking at areas of population who are more vulnerable than others. So, it's about looking at children's and young people's rights and how those are being upheld.



So, as you can see from the slide, we are probably likely to receive in the region of 45,000 cases across the EU. We think that's going to be in the region of 95,000 cases. Originally, before this week, we had estimated

that figure to be around 60,000, but with new figures which have just been published this week for International Data Protection Day, those are probably going to be around 95,000. Nevertheless, as you can see, with simple mathematical comparison, the UK is really receiving a huge bulk of the entire European complaints volume in our office. So, I wanted to point that out, because that's really interesting to us.

Of course, the other authorities around Europe are also facing huge increases in volumes, and they've had to manage that in their own way, so they're still receiving plus 50% or in some cases plus 60%, 70% of cases. For example, in Austria, there's a very small authority, who actually chairs the European Data Protection Board. They have been receiving in the region of one hundred complaints in the first month of GDPR and fifty-nine data breach notifications, and that would have been the same figure received in an entire year prior to GDPR, so what they're receiving in one month was what they would have otherwise received in an entire year. So, you can see there's a lot of pressure on data protection authorities here to step up to the new responsibilities.

The figures of the first five GDPR fines have been gathered together, and some of you might have seen those distributed on social media this week as well. Obviously, there's been a lot of publicity surrounding the French Data Protection Authority's fine against Google for around 50 million euros in relation to consent. There have also been fines from German authorities and Austrian authorities for other breaches of the GDPR as well.

In terms of the ICO's own Regulatory Action Policy, the Data Protection Act 2018 and GDPR, they have provided the background to our regulatory action policy in many ways. Our approach has to be that we take an effective, proportionate, and dissuasive approach. Those are the three key principles that are applied for application of the GDPR's corrective measures, and we apply a variety of different enforcement approaches corrective measures for that. That's all based on a risk-based approach, you can see those listed on slide seven. What I also wanted to emphasize is that our international enforcement cooperation capabilities have been really, really important to fine-tune and hone to make sure that GDPR works in the way that it was intended.

So, one thing to focus on—just to illustrate that enforcement approach under the GDPR— I'm going to take a very recent example from January 2019 in relation to SCL elections. Now this is an enforcement matter that we undertook under the old legislation, but I also wanted to get you thinking about what we may have done if we had applied the fines under the GDPR. The case itself has been applying the old legislation prior to the twenty-fifth of May, just because the breaches of the relevant laws

took place before the twenty-fifth of May, so were right to use the old law prior to the twenty-fifth of May. But the way in which we are looking as a modern regulator is, to quote our commissioner, "[w]herever you live in the world, if your data is being processed by a UK company, UK data protection laws apply."

And that's really, really important to bear in mind because the territorial scope in the GDPR since it came in from May last year really has expanded. We do have possibilities opened up to us at the ICO, and indeed at the other regulatory authorities around the EU, to be able to take actions against organizations if they meet certain criteria targeting individuals and so on.

In terms of the enforcement capabilities, we do have very clear powers and we do expect that companies meet their obligations. Where they fail to meet those obligations, the ICO can issue an enforcement notice compelling them to uphold those individuals' rights in compelling the organizations to meet their obligations and, as happened with SCL elections, the idea is that it is a criminal offense, and continues to be a criminal offense in the era of GDPR and UK accompanying legislation the UK Data Protection Act 2018, where an organization does not comply with our enforcement notice.

So, overall, we are showing our willingness as a regulator to use our increased powers. We haven't necessarily imposed a specific fine in the UK here yet on GDPR, but there are several cases in the pipeline which would allow us to consider doing so later this year. We have to make sure that we fulfilled all of our legal obligations as a UK regulator to be able to be in a secure position to be able to issue those kinds of fines, and so we need to make a sure we've done all of the legal checks necessary first. So those will be on their way**.** The willfulness of the commissioner to act has certainly been issued and certainly been heard.

So, using our new functions in practice, that could include things like assessment notices; we've already issued three assessment notices to the UK credit reference agencies recently. We have used our warning powers under the GDPR already, so that targets poorly performing controllers and where the data protection officer has noticed low level repeated breaches, though generally speaking, at the GDPR, the warning powers are used by us as the regulator only used for intended processing where the processing hasn't yet taken place. This makes it a great tool to be used by the authority in relation to data protection impact assessment that are submitted to us. We have already used warning powers in relation to a DPIA already**.**

High priority investigations have been earmarked to receive a kind of increased proportion of our overall resource under GDPR. So, we've created a special department to take on the full high priority investigations.

So once we have our general enforcement teams, we now have a high priority investigations team that can expedite particularly urgent work, and we have really boosted our compliance monitoring departments as well with a range of projects.

In terms of new horizons for our work, we've really heard the criticism of regulators over the years and tried to take that into account with a modern regulatory approach, so we've come up with our technology strategy, which was launched last year, due to be refreshed in 2021. We have identified three key areas for which we will focus our attentions in relation to a very fast-moving technological landscape. So, the first of those areas is site security, secondly, we'd be looking at the realms of AI, Big Data, machine learning, and that's certainly been a focus at the global level as well because we just had an international conference of more than 120 regulators last October which was also focusing on AI, ethics, and the future of Big Data there as well. We're making sure this all fits in with the global movement on regulation as well.

Finally, the third area we are looking at as part of our technology strategy is web and cross-device tracking. That technology strategy includes a variety of strategic goals, so we'll be increasing our own technology expertise. We'll be looking at how we can improve our guidance to the public and organizations on emerging tech issues, whether it's with the fin-tech sector, looking at Bitcoin, sharing our experiences and our understanding of these new emerging tech carriers with other authorities around the world, and to be able to engage in new areas of research, and build up new partnerships.

So how we can build knowledge exchange partnerships with other organizations who have expertise is definitely within our priority list as well. In terms of all of the objectives within this strategy, we definitely want to better understand the internet economy. We are very interested in how we can help mitigate risks in terms of internet harms, so we are currently working together with the UK national ministry (the Department for Digital, Culture, Media and Sport) on their approach to mitigating internet harm risks.

We also are placing a huge importance right now on practicing with innovation. You can have innovation and be privacy/data protection compliant. We fairly recently initiated special projects with support from various business, focused ministries, in terms of encouraging organizations in the private sector to develop their innovative approaches while also respecting privacy, but certainly not trying to dampen down that cutting-edge approach to innovation.

We're also improving our data protection impact assessment function, so we have a dedicated team looking at the data protection impact

assessments that are submitted to us, and understanding what the cutting edge of innovation is as a result of analyzing those data protection impact assessments and working out where developments are going in particular sectors.

To focus down on of our most high-profile publications of the last eight months or so, this is our Democracy Disrupted report. This is our focus, on the use of data analytics for political purposes and we have been very much in the media in many countries in relation to this investigation following revelations about Facebook, Cambridge Analytica, and its parent company SCL Elections, and many others in the data analytics ecosystem. It is very important for me to highlight here that it's not just about Facebook, it's not just about Cambridge Analytica. There is a whole ecosystem of influence throughout social media and other digital platforms that we are talking about and that we need to raise awareness in relation to the impact that influential power players are having on our democracy.

That includes looking, as I said at different digital platforms, with a very big focus on data brokers, the data broker sector, how researchers at universities are treating or handling personal data in relation to research that they may end up commercializing, how political parties and political campaigners at the grassroots level are using that personal data as well.

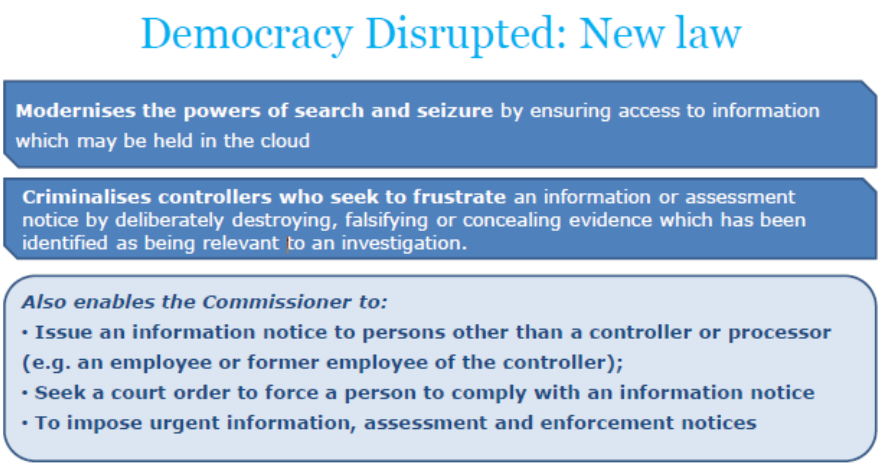
So, as you can see, across all of this, there's both a real importance for us to develop our international cooperation with our counterparts throughout key regions such as the US, Europe, and Canada, as well as working with key organizations at the UK level as well, such as the UK Electoral Commission, which governs the running for elections and the UK Center for Data Ethics and Innovation and working with them on specific projects.

The key recommendations, which are coming out of Democracy Disrupted, talked about the objective of making the data protection and electoral laws fit for purpose for our digital age, pulling that into the twenty-first century. We are often looked at in the UK, for example, as a cradle of democracy, but it looks like we have been really trailing in terms of how that applies to the digital environment and how these power players are really managing their presence and influencing individuals in the digital environment.

We want increased transparency for the use of data and for individuals to understand who is behind the political answer they're seeing on these digital platforms. We want to hold the online platforms themselves to account, and we want to be able to ensure the collaboration between regulators at the national and international level to combat to electoral interference. There's a lot going on also in Brussels at the

moment in the run up to the European elections later this year, so there are developments undertaken by the EU institutions to combat any undue interference in the running of those elections.

We've also placed a huge importance on digital literacy as well, so we are encouraging different actors to develop programs for digital literacy amongst the population. Democracy Disrupted has had a huge impact on the way in which the ICO conducts its activities. In the new law that came in last year, that is, the Data Protection Act 2018, we were able to gain modernized powers for search and seizure, ensuring our access to data which may be held in the cloud. We are also able to very soon criminalize controllers who seek to frustrate information or assessment notice where they deliberately destroyed, falsified, or concealed evidence which can be relevant to an investigation.



We also are able to issue an information notice to those individuals other than a controller. So, you can be somebody who used to work for an organization, and we can now issue an information notice to you. We can also seek court orders and impose urgent measures as you can see on the slide. In terms of the new understanding that this is engendered for our digital political ecosystem—this has really gained a lot of traction and a lot of new areas of work for us. At the height of our investigation, we had more than forty investigators working on this, drawing from across the organization, but this investigation has really helped us as a regulator overall to have a better standing in the digital age.

So electoral interference will be a global issue. It is an indeed fast-realized as a global issue, and it does require global solutions. There is a lot to be said about whether on the horizon you can see a global data protection treaty for example, or whether you could see new ways of

regulators cooperating with each other. But, indeed, the pressure is on for us to respond to these pressing problems for our democracy and society.

Moving on a little bit to the territorial scope expansion that we have in the GDPR. This is focused on shedding the light for those of you who may not be familiar with the broad principles behind this, and I should say at this point as well that the guideline on GDPR's territorial scope is being produced at the moment by the European Data Protection Board and is still under discussion, so we are well advanced with taking into account the results of the public consultation that was recently done in relation to this draft guideline, and there will be further news on that final guidance later this year.

Essentially, if you are a controller or a processor in the EU, you've got an establishment in the EU, then even if individuals you're targeting are outside the EU, you will be covered. If there is an inextricable link between the activities of an establishment in the EU with the data controller/processor who is located outside the EU, you'll also be covered.

In terms of targeting by a data controller or processor in the EU, if you're targeting data subjects, you're offering them goods or services, and they are in the EU, you will be covered and that includes also the monitoring of data subjects behavior, including processes such as profiling. There is a discussion ongoing about the future of processes in the EU who are used by non-EU controllers. I think that's still an interesting question that is being debated at the moment, certainly raised in public consultation, and you'll see more about that in the final guidance.

So, what is this European Data Protection Board which has been created by the new GDPR? What is its role? Why is it there? How has it evolved from what existed previously? Well, the board essentially replaces the old Article 29 Working Party. The old working party was the gathering of the same data protection authorities at the EU and the EEA level. So, the EU, the EEA, the European Economic Area, including Iceland, Lichtenstein, and Norway as well in the club, so twenty-eight plus three if you'd like. Also, the European data protection supervisor regulating data protection in the EU institutions and also the European Commission have a seat at the table as well.

This is all about promoting consistency and cooperation and the effective exchange of information and best practices to ensure that consistency is achieved. We have a whole new era of cooperation between us and all of the other supervisory authorities in the other twenty-seven EU countries, plus the three EEA countries. We have to work together as we did before on providing guidance, but we have to work together to provide what's known as a mutual assistance process to each other in relation to working on cross-border cases, and we have to resolve any

disputes between ourselves and other authorities who are concerned on a cross-border case. Luckily, no disputes have been raised to the board as yet, so we're working pretty cooperatively so far, which is positive news to report. It is important to emphasize that the board itself, even though it can issue legally binding decisions to a lead authority on a cross-border case, cannot enforce in individual cases itself.

The enforcement action is always taken by the authority leading the work at the national level, or in the case of places like Germany, at the state level, instead of a federal structure. In terms of guidance that's been produced by the board, we've got eighteen guidelines which were given the endorsement on the twenty-fifth of May. We've continued to work hard with our European counterparts on important features of the GDPR like certification and derogations to the international transfer rating which you can find in Article 49 of GDPR.

In the pipeline, so later in 2019, you can expect from us further work about the notion of contract in the context of free online services, as well as some guidelines on how individual data controllers or groups of data controllers such as trade associations and so on can produce codes of conduct, which build on the standard that GDPR provides. You can find all of that guidance on the EDPB website (www.edpb.europa.eu) and further news about any consultations which are coming up to inform the guidance in the pipeline as well. There are stakeholder consultations run by the EDPB every so often.

In terms of the output, there have been what is a relatively small proportion of cases in relation to the total receipt of cases that we are dealing with as individual authorities, so we've got in the region of 255 cross-border cases of which have been put on the books through our electronic case handling system in Europe at the moment. When you compare that to the figures that I showed you earlier, in terms of reaching in the region of ninety-plus thousand cases, that's a very, very small amount of cases which are cross border. However, it has required extensive efforts from all of us across the EU to be able to better cooperate together and to establish the new cross-border case handling systems.

I should also mention that there's no counting of cases here where the main establishment has been located in third countries because the cooperation role is different for the EDPB in those cases. In terms of the output of the EDPB in other ways, there's a whole variety of other things that it is doing as well. It is responsible for producing that general level of consistency, as I've already mentioned. One of the ways in which it's doing that is to produce opinions on lists of processing operations which require Data Protection Impact Assessment. We've been looking at the evolution of E-evidence laws, so foreign courts in particular requiring or

obtaining of evidence from other jurisdictions in Europe. We've been looking at the evolution of the E-privacy rules in Europe. Currently we have a directive on E-privacy that's evolving towards becoming a directly applicable regulation very soon.

EDPB output

Adopted:

- First general consistency exercise – EDPB opinions on national lists of processing operations which require DPIA
- Opinion on E-evidence
- Statement on E-privacy
- Statement on economic concentration
- Letter re ICANN/WHOIS
- EDPB opinion on EU-Japan Adequacy Decision
- View on Second Annual Joint Review of EU-US Privacy Shield

This slide shows a range of other things that we have been looking at in the EDPB. Notably also in relation to international transfers and, as you can see at the end, we've just completed the second annual joint review of the EU–US Privacy Shield as well.

Overall, the data breach notification rules for EDPB have been a deep interest to many. I think this slide is generally self-explanatory, but I do want to highlight, in particular, a couple of things that are on the left block and on the far-right block as well. If you are a data controller and you have no EU establishment under the scope of the GDPR, then GPDR does apply to you if the conditions for assessing any data controller are met, then we do recommend that you notify your data breach to the authority where your representative in the EU is. So, if you're unsure about which data subjects are impacted in different countries, go to the authority where your representative is. However, that doesn't mean to say you'll only end up with one corrective measure potentially against you**,** you could be subject to corrective measures from any of the authorities of the countries where the data subjects are.

I'd also point out that the representative can, but may not always, be liable for fines and penalties. So, there is a case-by-case approach to be taken here and I would recommend everyone to look at the territorial scope guidelines carefully when they come out later this year.

A final note on the EU–US Privacy Shield, as it has some Brexit relevance as well. I've got through most of this presentation without mentioning Brexit, which is quite amazing at the moment, but the Privacy

Shield does feature in the ICO's new guidance in relation to Brexit, particularly a no-deal Brexit situation. We issued that back in December, so just over a month ago. As many of you may know, this is the only US-received that the US received from the EU in relation to data adequacy in relation to which modified arrangements will apply. This is a specific EU–US arrangement, it is a partial adequacy finding. The UK government has been making arrangements for the Privacy Shield's continued application to restricted transfers from the UK to the US. There is further information available from the US government website, but what I would point out also is if the UK exits the EU without a withdrawal agreement, and a no-deal situation, then there is the possibility for UK businesses to continue to be able to transfer personal data to US organizations who participate in the privacy shield providing those organizations have updated their privacy notices or their public commitment to comply with the privacy shield to state that it covers the UK.

UK organizations who want to continue to make transfers to the US, if the UK exits the EU without a deal, will also need to check that the US organization adhering to Privacy Shield has updated its notice as well. So, there's due diligence required on both sides. You can have a look at our no-deal Brexit guidance which is available at our website for further details. You can also look at the EDPB's website for the very recently adopted opinion on the perspective that the board took as a group towards the second annual joint review of the Privacy Shield recently conducted last autumn. That was published in the last two weeks.

That concludes the presentation. I hope that you found that interesting and I'm more than happy to take a few questions if there's still time. The way in which we generally proceed is I can't comment on specific cases, but even if I can't answer your question directly, then I will most certainly endeavor to provide the answer later to colleagues at the university maybe as a follow-up. Alright, thank you very much. Back over to you professor and the team.

Steve Tapia: Thank you Hannah. We've got some questions I'm glad to say. I will do my best with handwriting. It's a very analog system. Does the GDPR give US citizens data subject access rights that they would not have in the US when their personal data is collected by a US controller but processed by a UK processor?

Hannah McCausland: Now, that's a very interesting question, and as I said during the presentation, that is currently being debated by the colleagues in the European Data Protection Board together with representatives from the ICO, so I can't give you a clear answer today because that line on that particular issue is live at the moment, so I would

really recommend you to look out for the territorial scope guidance which will be issued a little later in 2019.

Steve Tapia: Okay, and this is a follow-up question so it may be similarly contingent. What responsibilities do the UK processors have to the US data subjects when the US controllers don't cooperate?

Hannah McCausland: Okay, so what we've been doing at the ICO to get with our counterparts in Canada, in the US, and other leading authorities around the world is really promoting the way in which we cooperate with each other, to be able to uphold the individual's rights according to GDPR. I should say at this point as well actually that we have certain mechanisms of cooperation which I didn't go into detail during the presentation, but we do indeed have for example a Memorandum of Understanding with the US Federal Trade Commission which enables us to cooperate on cases, and we're currently updating that for all of the different scenarios that could happen under the GDPR. We've also got participation in a practical project with the US Federal Trade Commission again in relation to flagging cases that we are investigating and that we can let them know that we are investigating so that we can further our regulatory conversation together. We have a special mechanism to do that through what's known as the GPEN alert system. GPEN stands for the Global Privacy Enforcement Network, and that's a network of around seventy supervisory and regulatory authorities around the world. A relatively small proportion of those are involved in the alert system, but in the information sharing general platform of GPEN, there are many more involved. So concretely, we would be able to contact our US counterparts, we've got very good direct lines into them and discuss with them on individual cases. So, for example in relation to the Facebook, Cambridge Analytica data collection for analytical political purposes work, we very much had conversations with different regulators around the world including the US as well.

Steve Tapia: Hannah, you had mentioned, in the preamble to your talk about some of the hype I guess, for lack of a better term, my words not yours, around companies from the United States in particular news service providers being afraid of continuing to do business with you European clients. Can you talk a little bit more about that? In my experience as a practitioner that has worked with media companies, the business people generally like blue sky guidance, give me a big bright line, tell me what it is that I can do. I know that we've seen the *Chicago Tribune*, the *Washington Post* and other companies alter what's available to European subscribers because of a fear and maybe an irrational fear as to what the regulation requires of them. How would you speak to that? What advice can you give to somebody who has those kinds of clients in terms

of: is the fear unfounded, is there guidance, is there going to be guidance? At what point do we sort of know what the world's going to look like?

Hannah McCausland: Absolutely. Well there's a number of channels which we try to engage with organizations through, so organizations can indeed contact us via our help line, via our live chat, they can write to us via email to gain further guidance. We have a huge suite of guidance already on our website that they can refer to. We also refer to the guidance of the European Data Protection Board, and our own guidance as well. We're often trying to engage further, (for example, with this speaking engagement today!) with audiences in third countries as well. When I say third countries, I mean countries outside of the EU, EEA area. So, I really would encourage organizations not to panic about the new rules. The support is there for the questions that they may have. We have to take an approach of consulting with the stakeholders who would be impacted by our policies and we do that through the channels that I've already mentioned on a regular basis. I would say take it step-by-step. It hasn't produced the chaos that everyone thought it would after the twenty-fifth of May 2018. We are less than a year in. Obviously, there are lessons for everybody to take from the experience in the last eight months or so. We are constantly trying to improve our practice as well, so I'm also in listening mode to hear how organizations at the international level think that we could better engage as well. We certainly try to be flexible and try to listen on a number of fronts.

Steve Tapia: Okay. In your presentation you presented some numbers in terms of the number of complaints. Is there some correlation or causation as to why you've got an uptick in complaints of late other than the fact that you are finally able to be able to do your job and try to regulate?

Hannah McCausland: I think the principal reason is that we've had a number of very high-profile breaches by often global organizations which have really hit the media in a big way over the last few years. I think the sense of panic in some quarters and in the run up to the GDPR launch on the twenty-fifth of May last year meant the awareness was far, far higher. We invested a lot in a special campaign here in the UK called Your Data Matters to raise awareness of individuals about how their data was processed and how it should be processed according to the new laws of GDPR. So, a combination of factors I think raised awareness with organizations, whether that's through the media, and individuals bringing home the messages that they've been given by their management hierarchy at work about the new rules coming in. This has all made people sit up and take notice.

Steve Tapia: Okay. Let's see. I have a couple of specific, well actually three specific questions moving towards the criminal sanctions that are available. Who in the company has criminal liability for noncompliance with a compelled notice?

Hannah McCausland: That depends on the company. So, we'd have to look at individual case-by-case scenarios. There have been special developments here in the UK so directors of companies can now be held liable for noncompliance with the law. That is very, very new. We welcomed that development in the UK law recently, and I think the way in which the GDPR has heralded the way for accountability by organizations means that leaders at the very top of the organization now have to sit up and take notice. But particularly if you are an organization that requires a data protection officer because that data protection officer now has a relatively protected role under GDPR and has to report to the very highest levels of management in that organization, and so there is broad level attention now given to data protection compliance.

Steve Tapia: Okay, and in light of that, if you take the broad territorial claim of scope, have there been discussions or thoughts about how extradition might come into play for somebody that is criminally liable but is not within the confines of either UK or the EU?

Hannah McCausland: We'd have to look on a case-by-case scenario in relation to things like that. That's in very specific, serious cases. There may be situations where Mutual Legal Assistance Treaties come into to play in certain circumstances, but we really have to appreciate that the international enforcement cooperation legal landscape is a work in progress and there are certainly important discussions going on at the global level. For example, in the International Conference of Data Protection and Privacy Commissioners (ICDPPC) about how to advance that conversation as well. There are ways in which that could potentially be considered, but I think there's a long way to go on that part.

Steve Tapia: Got it. In the United States, it's always a fascinating question when legislation has sort of done our instituted piecemeal, how it relates to existing regulations. What's your view of the current existing relationship between the GDPR and the E-privacy regulation?

Hannah McCausland: This is very much a work in progress, the E-privacy regulation. The relationship between the two has been signaled in the GDPR already, there are clear signals laid out in the GDPR recitals for examples. However, the devil is in the detail; in fact, in this one and the way in which those two pieces of regulation will dovetail still needs to be clarified. I'm hoping for progress on that later this year.

Steve Tapia: Can you talk a little bit about the regulatory sandbox that the UK has implemented and what's the goals of the program, and what stage the program is in?

Hannah McCausland: Absolutely, I am happy to. So, actually there's been developments even this week on the development of our regulatory sandbox. We started talking about this broadly speaking last year. We would hope to open applications for the sandbox already at the end of April. So, what is the sandbox exactly? Well it's looked at as a special space for testing innovative cutting-edge products, interfaces. We are still shaping actually the way in which the sandbox will work, but we've already done a gathering of views last autumn on how organizations see the pros and the cons of developing such a sandbox.

This is very much a concept which is developed on the back of experience in other regulatory sectors. For example, by the Financial Conduct Authority here in the UK, they had a successful experience with the sandbox, and we hope to develop that successfully for the data protection regulatory space as well. It's really something which espouses the concept of insuring innovation whilst respecting privacy. So, we know that there are many emerging technologies out there where it's very difficult to understand which side of the fence they would fall on. Compliance or noncompliance with the GDPR.

We're talking about allowing ten organizations at the moment into a space where they can have a conversation with our authority about the projects that they're developing. How they will structure that conversation is still being finalized, but that could be for example in the form of informal advice given through kind of a test run of their product or service, we could participate for example in a joint workshop with them, and I don't want to use the concept of safe space too confidently here because what we're saying is that we would never *immediately* impose any kind of data protection enforcement notice against an organization that enters that space.

We would find out all of the facts first and make sure that our action was effective, proportionate, and dissuasive. It's certainly a space that is meant to encourage innovation as well, so we want to be able to encourage good data protection practice and compliance. What we would think about doing when an organization exits the sandbox program is to say that we didn't find any data protection issues with the product or service when they're exiting that program. So that would be the benefit, for them to say that they've gone through an assurance process with the ICO on that product or service.

So, as I've said, we're currently still defining that. We've got discussion papers out in the last couple of days actually to speak to the

different options which are available. We're really interested to hear, I think by the end of March, from any type of organization that might be interested in participating in that sandbox.

As I said, I think there's around ten spaces available so it is pretty limited at this beta-testing stage, but indeed, it's definitely an area which we've committed resources to, and we want to see how many kinds of applications we could expect out there. This is why we're testing the water with the beta phase so that we know whether we need to employ a larger resource to it or a smaller team, that depends. But the consultation is out there on our website and organizations, whether you're a tech startup or an innovation hub, they can already send us an email and ask more about that as well.

Steve Tapia: One final question as we bring to the close your time with us. What can we expect to see from ICO in the near future? You've explained the sandbox, but priorities, new positions, and other educational programs on the way?

Hannah McCausland: Absolutely. We intend to continue our engagement with all types of organizations to be able to advise them. We don't just see ourselves as a big stick regulator. There's that encouragement of organizations to really embody the responsible approach to accountability which is set out in GDPR. We are currently looking at how we can better reach businesses through our regulator's hub, which is a new team which has been set up, and we're working with other regulators to be able to get them encourage data protection and privacy through their approaches and their own engagement with business. So, we're getting others to repeat our messages as well as us directly communicating with business about how they can remain innovative while respecting privacy and data protection.

Steve Tapia: Hannah, I don't think we can thank you enough for such an excellent presentation, in addition to extending your day, and your week, well beyond anything that is reasonable.

Hannah McCausland: No problem.

Steve Tapia: You were absolutely fabulous, and we thank you.