Emma Bate speech
Conference 5RB
Wednesday 26 September 2018

Opening

Thank you to Conference 5RB for inviting me here to talk to you today.

This past year has been an exhilarating one both for me personally and for the ICO; I joined just over a year ago, from working as a private practice data protection lawyer. I don't think it's hard to imagine the many challenges both the ICO and myself, personally, have faced over the last 12 months.

We oversaw the biggest change to data protection in a generation with the dawn of the GDPR and the Data Protection Act 2018, we launched the largest data privacy case in the world with our investigation into Facebook and Cambridge Analytica, and we've significantly increased our staff, making us the largest data protection regulator in the world in terms of personnel and budget.

It's a tough year to beat.

GDPR

The new data protection laws in the UK have rebooted and strengthened our powers, obligations, and rights - a much-needed modernisation that gives us the right tools to tackle the challenges ahead.

It is still a principles-based law, but with plenty of new obligations, exemptions and remedies for us data protection lawyers to get our teeth into. As with anything new, it takes time to bed in, to get comfortable, and to become the new normal. And the GDPR is still finding its comfy spot.

But at the ICO we're already using our new strengthened powers under the GDPR: so far we have issued assessment notices, where we can require a controller or processor allow us to carry out an assessment of their processing, i.e. come in and undertake an audit. We have also issued an enforcement notice, where we can require a controller or processor to take steps to remedy any non-compliance with the GDPR. No fines as of yet under GDPR, and there are other cases working their way through our investigation and enforcement teams.

It's still early days and we will collate, analyse and publish official statistics in due course. But generally, as anticipated, we have seen a rise in personal data breach reports from organisations. Complaints relating to data protection issues are also up and, as more people become aware of their individual rights.

And we're expecting with more of everything so we've been busy recruiting more staff, taking us to around 650. With further increases expected and our enhanced technical capabilities, we are well on the way to becoming an innovative tech savvy regulator, but we have more work to do.

A key workstream for us, in bedding in the GDPR, is our work with the European Data Protection Board on producing guidelines. We are currently working on a number of areas, including the interpretation of Article 3 – the territorial scope of the GDPR and Chapter V of the GDPR which contains the restrictions on making international transfers of personal data.

We have already updated our ICO Guidance on International Transfers in line with the current EDPB thinking on this. I must give you a caveat that these EDPB Guidelines will be going out for consultation shortly, so the position may change.

But you may be interested to hear the current thinking regarding transfers. We have moved away from pure geographical considerations. A

transfer of personal data outside the EEA is not restricted by Chapter V of the GDPR if the data, when held by the non-EEA recipient, is still protected by the extra territorial scope provisions of the GDPR. The rationale being that no additional protection is needed as the GDPR still applies, so this is not a transfer outside of the protection of the GDPR.

You may also be interested to hear that we are also working on guidelines on the use of the Article 6 processing condition that processing is necessary for a contract, in the context of online services. Again that should be published over the coming months.

These aren't the only changes we're navigating. As Brexit approaches, we're planning for a number of scenarios, including a "no deal." We will be ready to provide practical advice for individuals and organisations should that be needed, in particular to help ensure the free flow of personal data between the UK and EEA.

Social media and Democracy Disrupted

We have recently conducted another round of public research that reveals that trust and confidence is lowest amongst social media companies.

Only one in seven (15%) people have high trust and confidence in social messaging platforms storing and using their personal information.

Given the amount of personal data held by social media platforms, this has to be very worrying. But surely also provides an opportunity for social media platforms to distinguish themselves from competitors in how they handle our data.

Technology should not mean organisations racing ahead of people's rights – remember, organisations don't outright own data: people always have some control over their own data.

We have a track record of regulating the online social media platforms.

Two which I have been involved in over the last 12 months are:

- First – you may remember there was an issue with WhatsApp and Facebook wanting to share user data after the Facebook takeover. If you are a WhatsApp user, you may not even have realised that it had updated its privacy policy to allow sharing customer data with Facebook.

  At the ICO we felt this was a situation where we had to step in, to stand up for the rights of UK citizens. After many discussions (which you can read in more detail in the Undertaking and Covering Letter which is available on our website) WhatsApp agreed to provide an undertaking that it would not share personal data with Facebook, as it had planned, until and unless it got its privacy statements and consents aligned with GDPR. WhatsApp had not actually shared any personal data, and with GDPR coming in imminently, WhatsApp and Facebook were in the process of reshaping their approach to data privacy.

- We also fined Yahoo! for its 2014 data breach, of 500 million international users.

AND of course we are responsible for overseeing Right To Be Forgotten disputes. This is the right to request that search engines, such as Google, delist you on European search results. Since 2014 the ICO has been grappling with these cases. The ICO has adjudicated and successfully resolved delisting disputes between individuals and the search engines, and we continue to do so under GDPR.

Democracy Disrupted?

We've all learned what happens when the tech giants don't take their data protection responsibilities seriously. Our Democracy Disrupted report looked at how personal data is used in political campaigns. It set out the ICO's policy findings and recommendations coming out of our data analytics investigation into political campaigning. This has also resulted in us issuing a Notice of Intent to issue a fine against Facebook of £500,000, and our investigation into Cambridge Analytica is ongoing. Under the Data Protection Act 1998 this is the largest fine we can issue.

Tailored, targeted digital campaigning through social media channels and other platforms is a relatively new and growing phenomenon in the world of elections. When we started the investigation, we couldn't have predicted where it would lead us. Our initial intention was to help inform people about the new ways their personal information was being used in political campaigns.

What is very different is the new techniques - the invisible processing – the behind the scenes' algorithms, analysis, data matching and profiling that involves people's personal information – which is then used to target individuals not just with campaign advertising but also with information, news stories and softer political messaging.

Some may ask why targeted campaigning on social media is any different from a political party knocking on your door to speak to you. A better comparison is that it's more like someone breaking into your house, rooting through your things, and then knocking on your door to talk to you.

We are not here to stop innovation or halt development of new techniques. We're excited about what the future may hold with AI and the internet of things and connected vehicles, for example. But future tech so often seems to have personal data at its core, our role is to ensure that it

is done lawfully, and that individuals are aware how their data is being used and what their rights are.

We are currently working on developing a Regulatory Sandbox, where we can work with innovators who are developing new data driven products, in a way which is compliant with the law. We currently have a public call for evidence open as to how we should operate this sandbox, and I would encourage any of you who might be interested to contribute to this. You can easily find it if you google ICO and sandbox!

Accountability and transparency are driving forces in the GDPR. The rules of transparency and fairness have not changed, but organisations are obliged to account for what they do, why and how they do it.

Organisations can't put a survey on Facebook and presume people understand what happens to any personal information they give away as part of that.

Across the world people have woken up to the importance of personal data and how it's used. When personal data has become the currency by which society does business, people do care. It goes without saying that people can't challenge organisations if they don't know what's happening, so it's all of our responsibility to make the public aware of their rights.

We know how difficult it can be to get people to engage with their privacy rights, and take the time to read a privacy policy. I can't say that I read privacy policies. Too often I am in a rush to sign up to the service to take the time to read a notice I know I can't change. But that approach isn't healthy or helpful in trying to encourage business to take my data privacy seriously.

But this is your sector's area of expertise. I'm sure if you put your creative minds to it you could come up with ways to interest your readers and your users in how you want to use their data. If a business can

create a TV advert to tell the world how lovely they really are, then why not harness that creativity and that voice, to explain and interest the public in privacy rights.

The media, data protection, and the ICO

Balancing rights and freedoms is not new for the media. But in a digital and data-driven age and post-Leveson world, the media face unique challenges.

I have a very good friend from my trainee days who now works in a TV production company, and she always has the best questions for me to ponder. For example, in a TV entertainment scenario, how do you investigate someone, while maintaining the element of surprise? It might spoil everything to present them with a privacy policy!

There is clearly a need to balance the fundamental rights to freedom of expression and to data protection and privacy in each case, and neither right automatically trumps the other.

Under the DPA 2018, the ICO will be preparing a journalism code of practice. This code will contain practical guidance for journalists and the press to consider when dealing with personal data. It will take into account the interests of individuals regarding data protection, alongside the public interest in freedom of expression and information.

We will also be publishing guidance setting out the steps which may be taken where an individual considers that a media organisation isn't complying with its data protection obligations. This guidance will cover: what can be complained about; how to make complaints; and who will deal with these complaints. Under the Data Protection Act 2018, this needs to be published by May next year.

In addition to this guidance, the ICO will also periodically carry out reviews looking at whether processing of personal data for journalism purposes complies with data protection legislation. Broadly speaking, these reviews will take place around every five years, and they will again weigh the interests of data subjects against the importance of freedom of expression. The first review won't be started for about 4 years.

We've intervened on two key cases involving the media this year, both of which I believe you will be hearing about in more detail later. I guess you could see it as one on the media side and one on the side of the individual.

The first was NT1 and NT2 v Google, which was a right to be forgotten case. Our intervention was in support of search engines having a lawful basis under the Data Protection Act 1998 to process sensitive personal data.

The second is Stunt v Associated Newspapers, which went to the Court of Appeal and a question has now been referred to the CJEU.

Mr Stunt's complaint relates to a number of articles published by Mail titles, and more specifically about the Defendant's acquisition, retention, and use of personal data.

Of course we took no view on the merits of Mr Stunt's complaints regarding the articles. Our intervention was in support of the position that any complainant against the media can find themselves without a remedy. The position had been that if the media was holding personal data for only journalist purposes with a view to future publication, any court proceedings had to be stayed. In our experience, time and again this has left a complainant without any form of judicial remedy, no matter the merits. To us, this felt that the balance was out, between freedom of expression and data protection and privacy rights, and the right to a judicial remedy.

The Court of Appeal found that the stay cannot be applied once the personal data has been published, even if there are plans for future publication. This is a change in interpretation of that provision, which is also in the DPA18. Previously the media could continue to rely on the exemption if it planned future publications with the same personal data.

The majority decided that this struck the right balance between freedom of expression and the right to privacy and data protection. It gives press freedom from data protection challenge while you are investigating, but that passes once you have published.

However, as a minority of judges thought that this still did not provide enough protection for the right to a judicial remedy, this question has been referred to the CJEU.

There are no simple answers to these types of question, where we are balancing fundamental rights and freedoms. So we welcome both the decision and the referral.

We're working to increase the public's trust and confidence in how their data is used and made available, and this year we launched our Your Data Matters campaign.

The media have the unique expertise and reach to engage with individuals, and is therefore well placed to support the ICO in our mission to educate the public about their data rights.

When only one in three people have trust and confidence in organisations using their personal data, we hope that others will too join us in our mission because data does matter.

Finally, my call to you at the beginning of this conference is twofold.

First, to look for the balance. You are often at the coal face of making decisions, of finding the right balance between the freedom of expression

and rights to privacy and data protection, and we appreciate how hard those decisions must be at times. I ask, that when applying data protection rules to your organisation, consider always how you might feel if you, or maybe your parents or children, were a data subject of the data at issue. When you are striving hard for the right to freedom of expression, remember to balance it against the importance of privacy to us all as individuals.

Second, to work alongside the ICO, so we can harness the huge creative power of the media and your expertise in communications, to strive to engage individuals in privacy rights.

So enjoy your day, and lets all make a pact to read more privacy policies.

Thank you.