VICTORIA HEWSON and JAMES TUMBRIDGE

iea

Who REGULATES the REGULATORS?

No.1: The Information Commissioner's Office

July 2020

IEA papers are designed to promote discussion of economic issues and the role of markets in solving economic and social problems. As with all IEA publications, the views expressed are those of the author and not those of the Institute (which has no corporate view), its managing trustees, Academic Advisory Council, or other senior staff.

About the authors

Victoria Hewson is Head of Regulatory Affairs at the Institute of Economic Affairs. A practising solicitor, she has specialised in commercial, technology and data protection matters across a range of sectors. In the Regulatory Affairs Programme she will be focusing on regulation and the role of regulators in the UK. Its first paper, 'Rules Britannia', was published in March 2020. She has published a number of papers for the IEA including 'Under Control - What HMRC can do to prepare and optimise customs processes for all outcomes' and 'Freedom to Flourish - UK regulatory autonomy, recognition, and a productive economy'. She writes regularly for *The Telegraph* and *City AM* and appears on television and radio to discuss trade and regulatory policy.

James Tumbridge is a partner of Venner Shipley, a specialist intellectual property firm. He has extensive experience in commercial litigation, intellectual property and alternative dispute resolution (ADR). James is particularly known for his government relations and data protection practice. He is one of the authors of the UK Data Protection Act 2018 that implemented the General Data Protection Regulation. He has extensive experience of regulatory compliance in matters of data protection in Europe and globally. He has advised on data compliance for politicians and political campaigns, advertising and promotions, and issues with data capture in virtual currency and customer data. He has been an ad hoc advisor to various UK Members of Parliament and Members of the European Parliament on this subject, as well as a range of IP and dispute issues. As a Chair of Police Tribunals, James has considered and ruled on data protection issues arising in the context of data and policy breaches. He has also trained three police forces on data compliance.

Contents

Summary	**4**
Regulator case study: the Information Commissioner	**6**
Assessment against impact assessments	**11**
Assessment against the Information Commissioner's objectives	**17**
Rule of law	**19**
A practitioner's view	**25**
Conclusion	**28**
References	**31**

Summary

- The Information Commissioner has wide ranging functions and powers. They are not always parameterised clearly in the relevant legislation. The Information Commissioner's reporting shows little evidence that objectives are being met, or even measured. The Parliamentary Committee responsible has not performed its scrutiny function of the Information Commissioner's Office (ICO) well and a forum appears to be lacking for detailed examination of its actions at a technical and legal level.
- In practice the current data protection regime is not working as had been foreseen by the European Commission in its impact assessment for the General Data Protection Regulation. The costs to businesses have been much greater than expected and there appear to have been negative effects on competition and investment. Many businesses are not fully compliant and some believe full compliance is not possible, suggesting that the Information Commissioner is not succeeding in its functions of promoting public awareness and understanding, and monitoring and enforcing compliance.
- There is insufficient oversight and review of fines and enforcement actions taken by the Information Commissioner. Challenging a decision is costly, there are serious procedural defects and imbalances, and the fines that can be levied are out of all proportion to the harm or loss caused.
- The Information Commissioner can issue guidance that is of uncertain legal effect but has serious consequences - and does so without producing impact assessments. This has negative consequences for the rule of law and accountability.
- The ICO is well regarded internationally and by business organisations for its role in data protection law and policy, but there are reforms that

could usefully be made to improve its accountability and effectiveness, while maintaining its independence.

Regulator case study: the Information Commissioner

This is the first in a series of case studies on regulators in the UK. It begins by summarising the legislative and practical functions, powers, funding and accountability framework of the regulator in focus, the Information Commissioner. This is followed by assessments of the operation of the Information Commissioner and the Information Commissioner's Office (ICO) against the economic impact assessments of relevant regulations carried out by government, and against the objectives set by the present Information Commissioner. The paper also examines the rule of law implications of the activities of this regulator. A leading practitioner in this field has contributed a view from first-hand dealings with the Information Commissioner.

The paper concludes by outlining options for how the role and functions of the Information Commissioner could be improved, to move towards a data protection framework that, through greater certainty and proportionality, will support economic growth and innovation, while still protecting the rights and interests of individuals.

Who	The current Information Commissioner is Elizabeth Denham. The Information Commissioner is supported by a Non-departmental Public Body – the Information Commissioner's Office (ICO). The Information Commissioner's 2018/2019 Annual Report states that the ICO has a workforce of more than 700.

Purpose/ establishing legislation	First established by the Data Protection Act 1984 as the Data Protection Registrar, the principal legal base for the Information Commissioner and her Office is now the Data Protection Act 2018 (DPA). The Information Commissioner is an independent official appointed by the Crown and the Information Commissioner's Office is an Executive Non-departmental Public Body. The ICO is the independent supervisory body mandated for member states by the EU General Data Protection Regulation (GDPR). Functions of the Commissioner include monitoring and enforcement of relevant parts of the DPA; promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, and awareness of controllers and processors of their obligations; and advising Parliament, the government and other institutions and bodies on the protection of individuals' rights and freedoms with regard to processing of personal data. The Information Commissioner also has powers and responsibilities under the Freedom of Information Act, the Privacy and Electronic Communications Regulations (PECR), the Environmental Information Regulations, the eIDAS Regulations and the Re-use of Public Sector Information Regulations. This case study is focused on the DPA/GDPR and PECR. The legal responsibilities of the Information Commissioner have been interpreted by the Information Commissioner as requiring the following strategic goals: 1. To increase the public's trust and confidence in how data is used and made available. 2. Improve standards of information rights practice through clear, inspiring and targeted engagement and influence. 3. Maintain and develop influence within the global information rights regulatory community. 4. Stay relevant, provide excellent public service and keep abreast of evolving technology. 5. Enforce the laws we help shape and oversee. 6. To be an effective and knowledgeable regulator for cyber-related privacy issues. And the following values: • Ambitious – working boldly, ready to test boundaries and take advantage of new opportunities; working with a sense of genuine urgency, continuously improving when striving to be the very best we can be. • Collaborative – working towards achieving our goals, supporting one another whilst seeking and sharing information and expertise and working effectively with a range of partners to achieve our collective objectives. • Service focused – working impartially and ethically to provide excellent services – continuously innovating to remain relevant to the environment we regulate.

Accountability	The ICO is sponsored by the Department for Digital, Culture, Media and Sport (DCMS) and a minister in that department is responsible to Parliament for the ICO. The Information Commissioner reports to the DCMS Select Committee on its agreed key performance indicators. The GDPR requires national supervisors to be free from external influence and not subject to instructions, so a Management Agreement is in place between the ICO and DCMS to set out the Information Commissioner's priorities, funding and engagement, financial controls and governance framework. This is intended to allow the Commissioner to work independently within a broad framework of accountability. Enforcement notices can be appealed to a tribunal and ultimately the courts, and the Information Commissioner's decisions can be judicially reviewed in the courts.
Rulemaking power	The functions of the Information Commissioner under the DPA include preparing codes of practice for: • data sharing • direct marketing • age appropriate design • data protection and journalism The Commissioner also has a duty to advise Parliament and government and other institutions and issue opinions. Under the general functions of promoting awareness and understanding, the ICO produces guidance on the GDPR, DPA, PECR and FOIA. Such guidance and the Codes of Practice are not directly binding but compliance with them will generally be seen as evidence of compliance with the associated legal obligations. Courts and tribunals are obliged to take the statutory Codes of Practice into account in determining matters that come before them.
Price-setting power	None

Enforcement powers	Under the GDPR and the DPA the Information Commissioner has the powers to: • carry out data protection audits • require information from controllers and processors and access to their premises • issue enforcement notices and fines of up to €20 million or 4 per cent of the company's global annual turnover • bring criminal prosecutions The Information Commissioner also has powers of investigation and can impose fines under other laws, including the ability to fine up to £500,000 under PECR. The ICO is seeking additional powers under the Proceeds of Crime Act such as the right to apply to the court for Restraint Orders and Confiscation Orders, powers of cash and asset seizure, detention and forfeiture from premises.
Funding	The ICO is funded by a grant in aid from DCMS. Some of the cost of the grant is offset by fees paid by data controllers. Current fees are: • Tier 1 – micro organisations. Maximum turnover of £632,000 or no more than ten members of staff. Fee: £40 - Fine for not paying: £400 • Tier 2 – SMEs. Maximum turnover of £36million or no more than 250 members of staff. Fee: £60 – Fine for not paying: £600 • Tier 3 – large organisations. Those not meeting the criteria of Tiers 1 or 2. Fee: £2,900 - Fine for not paying £4,000 • Failure to pay the fee is a civil offence under the GDPR In 2019 the grant in aid from DCMS was £4.6 million. Fines issued by the Information Commissioner are returned to the Treasury Consolidated Fund, not retained by the ICO. The Commissioner has responsibility for determining the pay and conditions of ICO staff. The Management Agreement states that 'Pay and conditions are expected to be affordable, proportionate and responsible'. The ICO is currently in a period of 'pay flexibility' allowing the Commissioner the ability to determine levels of pay necessary to maintain the expertise that the ICO needs to fulfil its functions. In 2021 the ICO will revert to being subject to HMT's standard public sector pay policy guidelines. The Commissioner's salary is set by DCMS at £160,000. In 2018 Elizabeth Denham was given a special, additional allowance taking her salary to £180,000. The Management Agreement sets out financial controls, reporting requirements and spending limits.

EU element	GDPR is a directly applicable regulation but gives some flexibility to member states to implement derogations. PECR implements an EU Directive. The DPA also implements the Law Enforcement Directive. The UK will retain the substance of all of these EU laws by way of the Withdrawal Act 2018 and the Withdrawal Agreement Act 2020 in what will become, at the end of the Transition Period, the UKGDPR. The GDPR sets out requirements for the constitution and operation of data protection authorities in member states. These include: independence – that members of the authority 'remain free from external influence… and neither seek nor take instructions from anybody' and tasks including monitoring and enforcing the regulation, promoting awareness and understanding, advising parliament, government and other bodies, handling complaints and conducting investigations and 'monitoring relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices', as well as more routine tasks of administering the operation of the regulation in practice. The Withdrawal Agreement (implemented in the Withdrawal Agreement Act) also requires the UK to apply the GDPR and all other EU data protection laws to the processing of personal data of individuals outside of the UK when the data was collected before or during the Transition Period or is processed pursuant to the Withdrawal Agreement. The GDPR has extra territorial effect, so it applies to an organisation anywhere in the world that processes the personal data of individuals in the EU if it has an establishment in the EU, or even if it has no presence in the EU but offers goods and services to people in the EU or monitors their behaviour. The ICO will have no role in overseeing this aspect as it will cease to be an EU supervisory authority under the GDPR, but as the UK will be retaining the extraterritoriality in its domestic version of the GDPR, the ICO will be expected to monitor and enforce the compliance of overseas companies processing UK personal data. The GDPR prohibits the transfer of personal data from the EEA to third countries unless the receiving country has been deemed by the Commission to provide an adequate level of protection for personal data, or other 'appropriate safeguards' are in place. Appropriate safeguards can include approved contract terms between sender and receiver, and a limited number of other mechanisms that are untested or costly to put in place. The UK is seeking an adequacy decision from the EU, and the EU indicated in its negotiating mandate that it would work towards this. The UK has indicated in its negotiating objectives for the future relationship that it will 'have an independent policy on data protection at the end of the transition period and will remain committed to high data protection standards'. Rather than looking to maintain the participation of the Information Commissioner as the supervisory authority for GDPR purposes the UK objectives envisage 'continued cooperation between the UK Information Commissioner's Office and EU Member State data protection authorities, and a clear, transparent framework to facilitate dialogue on data protection issues in the future'.

Assessment against impact assessments

The European Commission and the UK's Ministry of Justice (MoJ) and DCMS all carried out impact assessments of the GDPR. The Commission concluded that the regulation would be a de-regulatory measure with 'drastic' reductions in red tape. The British government was sceptical of this and commissioned the MoJ to carry out its own assessment of the draft GDPR. The DCMS impact assessment came later and focused on the costs and benefits of the way the derogations under the GDPR were to be implemented in the UK. It is notable that the policy options analysed by the UK departments and the Commission did not include a de-regulatory option – the only options were variations on the existing baseline regulation, the Data Protection Directive 1998, and its national implementation.

Because the GDPR has fundamental rights objectives as well as economic ones, it is difficult to monetise its benefits. However, this does not mean that the effectiveness of measures aimed at protecting fundamental rights cannot be questioned. As Milton Friedman famously pointed out, it is a mistake to judge policies by their intentions rather than their results, so the ICO and data protection legislation should not get a free pass because protecting privacy is an important and worthy objective.[1] A consideration of privacy and protection of personal data as fundamental human rights is beyond the scope of this paper, but even in the EU's formulation under the Charter of Fundamental Rights, privacy and data protection rights are not absolute. They must be weighed against other considerations such as the right to carry on a business, the right to free expression and

1 In fact, there is evidence to suggest that personal data is at more risk from some requirements of the GDPR. For example, subject access requests are vulnerable to bad actors being able to access all of an individual's data.

legitimate interests of businesses and society in general in innovation and competition in services that involve processing personal data. From the impact assessments carried out by the Commission and by the UK government there is little evidence that such balancing factors have been sufficiently accounted for.

The Commission Impact Assessment accompanying the draft GDPR in 2012 (European Commission 2012) defined three problems with the status quo under the 1994 Data Protection Directive: barriers for business due to fragmentation, legal uncertainty and inconsistent enforcement; difficulties for individuals to stay in control of their personal data; and gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters. The policy options it considered were, broadly: 1. improve the functioning of the existing laws with better tools for interpretation, self-regulation, cooperation and standardisation; 2. legislative amendments to address gaps in the current framework and effect some increased harmonisation; and 3. detailed harmonisation and rules at EU level (including detailed rules for specific sectors) with centralised enforcement and harmonised sanctions and redress mechanisms. The preferred option, enacted as the GDPR, was option 2. The Commission estimated that this option would reduce the overall administrative burden on businesses by about €2.3 billion per annum, on the basis that additional costs associated with appointing data protection officers and dealing with data subjects' rights would be offset by savings from reducing fragmentation and notification requirements.

It noted that 'privacy and data protection can increase consumer confidence' which 'could enable European companies to capture the market share of Europeans who do not shop online because of a lack of trust'. This option could also 'act as a stimulus to innovation'. It also struck a protectionist note: 'non-EU companies which do not have appropriate standards will be limited in their ability to operate within the EU'.

The UK government believed that the Commission 'overestimated the benefits from one single law and … failed to take into account many of the new compliance costs in its headline figure by focusing purely on administrative burdens' (Ministry of Justice 2012). The MoJ therefore produced what it considered to be a fuller summary of the costs and benefits and their impacts in the UK. It found that the Commission had overestimated the benefits, underestimated the costs and not included policy costs in its impact assessment, and found the GDPR would have

a net present value in the UK of –£2.1 billion over the 14 years from its implementation.

The Commission's striking findings that the GDPR would result in a reduction in red tape and compliance costs have been proved woefully wrong, and the MoJ's doubts have been vindicated. The International Association of Privacy Professionals estimated that Fortune's Global 500 companies would spend roughly $7.8 billion in order to ensure they are compliant with GDPR.[2] In the UK, FTSE 350 companies are estimated to have spent over £1 billion on compliance,[3] spending up to 40 per cent of their legal budgets on GDPR in the run up to it coming into force.

As the estimated savings were based principally on the elimination of data controller notification requirements and the introduction of one-stop-shop supervisory mechanisms that would reduce the costs of fragmentation for (the minority of) businesses that trade cross border, this is not surprising. The Commission's impact assessment seemed to neglect the effect on small businesses that do not operate material cross-border data flows and businesses that, while not primarily digitally focussed, rely on data to develop and innovate, such as manufacturing businesses. They also materially underestimated the extent of the new burdens and risks introduced by the legislation, backed by the possibility of heavy fines, leading to possible over-compliance.

The offsetting gains from increasing participation in digital markets are also questionable. A report by London Economics, commissioned by DCMS in an effort to 'quantify the benefits arising from personal data rights under the GDPR', notes that (Godel et al. 2017):

> the scenario described by [the European Commission], where not implementing the GDPR … would 'counteract the key performance target of the Digital Agenda for Europe for 50 per cent of the population to buy online by 2015' has not come to pass: the EC's own data shows that the target had been achieved by 2015: over the last five years, the number of European citizens ordering goods and services online has increased by 13 percentage points, to 53 per cent.

2 'Global 500 companies to spend $7.8B on GDPR compliance', IAPP, 20 November 2017 (https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/).

3 'GDPR preparation has cost FTSE 350 businesses around $1.1 billion', Consultancy UK, 23 May 2018 (https://www.consultancy.uk/news/17226/gdpr-preparation-has-cost-ftse-350-businesses-around-11-billion).

Similarly, the MoJ's conclusion that an increase in the use of internet services would be a potential benefit of enhanced protection of personal data, according to London Economics:

> cannot be easily reconciled with a situation in which internet use in the UK has been growing consistently and is already very widespread: The internet was used daily or almost daily by 82 per cent of adults in Great Britain in 2016, compared with 78 per cent in 2015 and 35 per cent in 2006. In 2016, 89 per cent of households in Great Britain had internet access, and 77 per cent of adults bought goods or services online.

Evidence from other jurisdictions seems to confirm that a lack of trust in data protection regulation does not hold back data driven transactions:

> Europe as a whole lags behind the USA on a broad range of digital economy indicators, which suggests that different data protection regimes are compatible with highly developed digital markets. The evidence that the US combines lower trust in the domestic data protection regime with a higher level of digital development does not support the view that the European digital economy suffers in comparison *because of* an insufficiently strong regulatory framework.

London Economics also carried out an exercise to find out how much consumers value certain rights under the GDPR. To mitigate the known issue of the 'privacy paradox' (Norberg et al. 2007) where consumers claim to attach a very high priority to protecting their privacy but in practice freely participate in transactions that involve providing personal data, they constructed a choice experiment based on three consumer products. The results of the tests indicated that consumers are 'willing to forego savings of roughly 5 per cent to 10 per cent on weekly spending on shopping, monthly spending on electricity or monthly spending on health insurance in order to have the rights enshrined in the GDPR'. According to the report, which was cited in the DCMS impact assessment, 'this large valuation indicates that individuals are generally happy with the package of rights they have and that they should be compensated significantly for these rights to be taken away'. However, a more critical reading of this data would surely have been sceptical of these very high valuations. It could also have provoked the question, taking the results of the test at face value, of why we need regulation to enforce these practices when, with such a high

valuation, surely the market would react to deliver high privacy services to consumers willing to pay for them.

Far from stimulating innovation and competition in digital services (other than, as the Commission impact assessment cheerfully predicted, in data protection consulting) the early signs since implementation of the GDPR are that concentration in digital markets has increased, to the benefit principally of Facebook and Google (Johnson and Shriver 2020). Investment in technology start-ups fell in the aftermath of GDPR coming into effect, which could result in a yearly loss of up to 29,000 jobs in the EU (Jia, Jin and Wagman 2018). Combined with the direct compliance costs, the costs of innovation and investment foregone are serious and indicate that the GDPR is operating in opposition to the policy priorities of the UK and the EU in respect of innovation and competition in the digital economy.

In its first evaluation report on the regulation the European Commission found it 'has successfully met its objectives of strengthening the protection of the individual's right to personal data protection and guaranteeing the free flow of personal data within the EU' (European Commission 2020). The report does not cite any data on compliance rates or improvements in security, investment or innovation, citing more use of corrective powers (such as fines) by national regulators and a survey of EU citizens showing high levels of awareness of the GDPR and national authorities as evidence that rights are better protected. Although one of the main objectives of the GDPR was to reduce fragmentation, the report considered that fragmentation in implementation and enforcement is still a problem and further harmonisation may be required. Notwithstanding all of the available data on the costs and effects of the GDPR on investment and competition in the two years since it came into force, the Commission considers that its provisions 'have the potential to lower the barriers to entry for businesses and open the possibilities for growth based on trust and innovation'. The difficulties of small and medium enterprises are acknowledged, but waved away with suggestions of more support with compliance.

The DCMS impact assessment recorded as an objective maintaining alignment with the EU so as to facilitate cross border data flows. The EU has made clear that an 'adequacy' decision that would allow personal data to be transferred from the EU to the UK without further protection is not certain to be given, and the prime minister has emphasised that the

UK will be asserting 'full sovereign control over … data protection'.[4] It would be advisable to carry out an assessment of the costs and benefits of continuing with the EU's GDPR framework, including the possible benefits of reforming the regime and the costs of not achieving an adequacy decision.

4 'Prime Minister Boris Johnson's speech in Greenwich', 3 February 2020 (https://www.gov.uk/government/speeches/pm-speech-in-greenwich-3-february-2020).

Assessment against the Information Commissioner's objectives

In her 2018/2019 Annual Report, the Information Commissioner reported against her strategic goals. The report includes data on enforcement showing increases in numbers of compliant businesses and reports, and describes cases of investigative action and fines, but there is little to demonstrate whether data protection laws are actually being complied with. Reports from elsewhere indicate that 30 per cent of firms are not compliant, that there is widespread confusion as to what the regulation requires, and that GDPR fatigue has set in with the overload of guidance and information.[5]

The reported achievements on increasing public confidence rely on increased numbers of complaints and calls to the ICO, and a survey showing an increase in trust and confidence over time, but the Information Commissioner notes that further research is needed to establish whether this is caused by regulatory interventions or other factors. Data from the London Economics report mentioned above suggest that increasing trust and confidence is in fact part of a longer-term trend. In 2018 the ICO revealed that it had been receiving 500 reports by telephone a week since GDPR came into force. Although in her annual report, the Information Commissioner considered an increase in complaints and other interactions with the public to be a positive, indicating that the objective of increasing

5 '30% of European businesses still not GDPR compliant', Consultancy UK, 26 July 2019 (https://www.consultancy.uk/news/21951/30-of-european-businesses-still-not-gdpr-compliant).

public trust and confidence was being met, in fact a third of reports to the ICO were found to have been unnecessary.[6]

Of the Codes of Practice that the Information Commissioner is required by the Data Protection Act to publish, only one has been finalised. The Age Appropriate Design Code (AADCOP)) was laid before Parliament in June 2020 and will come into force 12 months after it passes Parliament's draft negative resolution procedure. While the other three have not yet been published or are undergoing consultation, the Information Commissioner wishes to extend the role to include 'protecting democracy'. In 2019 the Information Commissioner issued recommendations 'designed to restore the trust and confidence of electorates and the integrity of the electoral process'. It could be argued that this is beyond the scope of the objectives of the Information Commissioner and falls more obviously under the remit of the Electoral Commission, and of Parliament itself. The very broad scope of the 'tasks' of the Commissioner as an authority under the GDPR could conceivably include such guidance under the headings of promoting public understanding and awareness, and advising bodies and institutions on matters related to personal data processing. The scope of these tasks could benefit from review after the end of the Transition Period, when the UK is no longer bound to the EU GDPR, with a view to preventing gold plating and policy freelancing by the Information Commissioner.

The Information Commissioner reports to the DCMS Committee. However, in practice this committee has been focused on newsworthy campaigns that accord with the particular interests of members, rather than more prosaic scrutiny of the ICO's performance against its statutory functions and own stated objectives. While Parliamentary enquiries into wide ranging topics such as disinformation and abuses in electoral processes (which have taken up a large part of the time of the DCMS Committee in recent years) are important, a forum appears to be lacking for detailed examination of the activities of the Information Commissioner and the ICO, focused on the fulfilment of the Commissioner's statutory functions at a technical and legal level.

6 'Companies "over-reporting" data breaches as ICO takes 500 calls per week', IT Pro, 13 September 2018 (https://www.itpro.co.uk/information-commissioner/31912/companies-over-reporting-data-breaches-as-ico-takes-500-calls-per).

Rule of law

Guidance and Codes of Practice produced by the ICO can have material implications for businesses and organisations (public and private sector) which are subject to data protection legislation. In the foreword to the Age Appropriate Design Code of Practice (AADCOP), the Information Commissioner stated 'This code will lead to changes that will help empower both adults and children', a troubling assertion in respect of a Code of Practice pursuant to a mandate to issue guidance towards compliance with the law, not make new rules. 'This code will lead to changes that UK Parliament wants', she continued, and the Age Appropriate Design Code certainly does make changes, including introducing a duty on private operators to comply with the UN Convention on the Rights of the Child, but if this is the case then surely Parliament could have legislated for such changes rather than leaving them to an unelected body that does not have law making power.

Parliament did not intend that the Information Commissioner should have the power to make substantive rules, only to issue guidance (as set out in section 123 of the Data Protection Act 2018). Failure to comply with codes of practice issued by the Commissioner expressly do not make a person liable to legal proceedings, however both the AADCOP and the draft Direct Marketing Code of Practice published in March 2020 present guidance as law, and good practice recommendations as guidance on compliance with law. For example, while acknowledging that it does not create law, the AADCOP states 'If you do not follow this code, you are likely to find it more difficult to demonstrate your compliance with the law, should we take regulatory action against you'. However, it has been noted

that much of the AADCOP has no basis in law.[7] Similarly, the draft Direct Marketing Code of Practice states 'We will monitor compliance with this code through proactive audits … and enforce the direct marketing rules in line with our Regulatory Action Policy. Adherence to this code will be a key measure of your compliance with data protection laws. If you do not follow this code, you will find it difficult to demonstrate that your processing complies with the GDPR or PECR', whereas in fact much of the draft Code reflects optional (but recommended) good practice on matters seen to be desirable by the Commissioner. As noted elsewhere in the draft, 'It explains the law and provides good practice recommendations'. Such lack of clarity between what the Commissioner considers 'good practice' and what it considers to be the binding legal requirements contributes to uncertainty as to the meaning and effect of the law and to over-compliance by data controllers and processors.

There are also substantive problems with guidance produced by the ICO adopting contestable positions. For example, interpretations of PECR in the existing and draft updated Code of Practice on Direct Marketing that include non-commercial communications as direct marketing, but do not make the exception from obtaining opt-in consent available to them, constrain the ability of charities, political parties and movements, and public services to communicate electronically in a compliant way. Such interpretation is arguably at odds with the underlying Directive[8] but the ICO has persisted with it, putting charities and the not-for-profit sector at a disadvantage. The draft Code of Practice on Political Communications (published by the Information Commissioner in 2019) adopts a definition of 'political campaigning' that undermines the definition of (and safeguards for) democratic engagement in the Data Protection Act itself. The AADCOP will impose serious burdens on all e-commerce providers and website operators and could impact on the user experience of all internet users. However, none of this guidance was subject to an impact assessment by the ICO. When the Code was laid before Parliament in June 2020, the explanatory memorandum stated:

> [T]he Secretary of State has asked the ICO to undertake an assessment of the Code's economic impact in order to inform the package of support to industry, which will minimise the risk of

7 'What do you need to know about the ICO's Age Appropriate Design Code?', Brodies LLP, 23 January 2020 (https://brodies.com/blog/ip-technology/what-do-you-need-to-know-about-the-icos-age-appropriate-design-code/).

8 See Recital 40 of Directive on privacy and electronic communications.

> disproportionate burdens on small businesses. The assessment of economic impact will be completed before the Code has completed its parliamentary passage.

The ICO said in response that it would be 'pulling together our existing work on the benefits and the costs of the code to assess its impact. This will inform the discussions we have with businesses to help us develop a package of support to help them implement the code during the transition year'. Aside from the particular interpretation that the ICO has taken in fulfilling the request of the Secretary of State, an impact assessment that will only be used to assist in implementation of the Code will not achieve the main purpose of a regulatory impact assessment: analysis of the costs and benefits of the measure per se, and whether one outweighs the other, which must surely be of interest to MPs when they consider the Code.

The Commissioner has been criticised[9] for adopting the profile of an activist in pursuing online harms regulation and measures to protect children that amount to content regulation. Proclaiming in an interview in the *Sunday Times*[10] that 'The time for self-regulation - especially from large platforms - is over', could be seen as overstepping the boundary between expert regulator and politician in this contested topic. Making speeches and presenting evidence on fake news and disinformation at international conferences on 'unmasking and fighting online manipulation', cited as evidence of meeting the objective of increasing the public's trust and confidence, could also be seen as taking a partisan side in the so-called 'culture wars' and certainly as a lower priority in the face of massive non-compliance and confusion as to the operation of the GDPR.

9 'Tech policy is no place for hero fantasies', WebDevLaw, 18 July 2019 (https://webdevlaw.uk/2019/07/18/tech-policy-is-no-place-for-hero-fantasies/).

10 'The guardian angels making the internet a safer place for children', *The Times*, 2 June 2019 (https://www.thetimes.co.uk/article/the-guardian-angels-making-the-internet-a-safer-place-for-children-r9c2c5v79).

The Information Commissioner's dual role in giving advice on compliance with the law as products and services are developed, and then monitoring and enforcing the law in respect of such products and services has been called into question by the Parliamentary Joint Committee on Human Rights. The Committee heard evidence from the Commissioner on the contact tracing app developed by NHSX (the technology wing of the NHS). The Information Commissioner has been working with NHSX and advising them on their Data Protection Impact Assessment (DPIA). DPIAs are required by data protection law when an operator proposes to undertake processing of personal data that poses a risk to the rights and freedoms of individuals whose personal data is involved, and in high-risk cases the data controller must consult with the Information Commissioner. MPs expressed concern that being involved in advising on the development of the app could be prejudicial to the ICO's future role in monitoring and enforcing NHSX's compliance with data protection and privacy laws.[11] The Information Commissioner acknowledged the concern but explained that this is the role prescribed by law. In a subsequent letter to the Committee, she stated that 'clear governance systems and processes underpinning the way our regulatory advice is provided' allow the Information Commissioner to 'retain independence as a regulator in order to make appropriate decisions around audit, investigation and enforcement'.

The Committee recommended that new legislation be passed and 'an independent body, such as a Digital Contact Tracing Human Rights Commissioner' be created to oversee the compliance of digital contact tracing (House of Commons and House of Lords Joint Committee on Human Rights 2020). These recommendations are arguably misconceived, as the law already provides for most of what the Committee wishes to 'enshrine in law' and new law risks adding to the confusion. It is however a serious criticism of the way the Information Commissioner's functions have been formulated and developed that a distinguished committee of MPs and peers considered that it is not in a position to oversee such an important and controversial development.

11 Oral Evidence to Joint Committee on Human Rights, at Question 17 (https://committees.parliament.uk/oralevidence/334/pdf/).

The ICO's powers and approach to fines also threaten the rule of law. The ability to impose huge financial penalties, out of all proportion to any harm suffered,[12] in itself does not respect natural justice and gives the regulator immense discretion. In its impact assessment the MoJ noted that the fines in the draft regulation (which were set at lower limits than those provided for in the version of the GDPR that was enacted) would be a cost to business, even to those not subject to fines, because they are 'disproportionate to the harm caused [so] are expected to lead to data controllers spending a disproportionate amount of resource to ensure technical compliance'.

The process by which enforcement action is taken is opaque and inconsistent. Companies which have been hit with the highest fines to date (British Airways, Marriott Hotels and Facebook) have been able to use the financial and legal resources available to them to negotiate with the ICO. In the case of Facebook, after it raised issues of bias and procedural unfairness in its appeal against a fine of £500,000[13] the Information Commissioner settled the matter out of court and allowed Facebook to pay the fine without admitting liability. In 2019 the ICO announced intentions to fine British Airways £183 million and Marriott £99 million. The finalisation of the fines, and conclusion of the regulatory action against them, now seem to have been delayed until August 2020. This was announced by the Information Commissioner in an online conference, in another departure from the formalities of transparency and clarity.[14] It has been suggested that the delays could have arisen because the ICO is not in a position to fight the legal firepower that these large corporations will be able to bring to their appeals. The ICO has already shown in the Facebook case that it is not able or willing to defend itself.[15] Smaller businesses will not be able to bring such leverage to bear on their interactions with the regulator and even for larger businesses the uncertainty

12 It is notable that in the case of the record fine that the Information Commissioner intends to impose on BA, there is no record of any individual suffering a loss or of any fraudulent transaction occurring.

13 'Preliminary Issue Ruling', First Tier Tribunal, General Regulatory Chamber (Information Rights) (https://panopticonblog.com/wp-content/uploads/sites/2/2019/07/033-270619-Preliminary-Issue-Ruling-Facebook-Ireland-and-Inc-EA20180256.pdf).

14 'ICO appears to announce yet further delays to BA and Marriott investigations', Mishcon de Reya, 12 May 2020 (https://www.mishcon.com/news/ico-appears-to-announce-yet-further-delays-to-ba-and-marriott-investigations).

15 'UK data watchdog kicks £280m British Airways and Marriott GDPR fines into legal long grass', The Register, 13 January 2020 (https://www.theregister.co.uk/2020/01/13/ico_british_airways_marriott_fines_delayed/).

and lack of transparency, as well as the legal costs involved, are damaging. In light of all of this, the prospect of the Information Commissioner and the ICO having the even greater powers they have requested[16] under laws combating financial crime may raise concerns for the Home Secretary.

16 'ICO call for views on the application for powers under the Proceeds of Crime Act' (https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-the-application-for-powers-under-the-poca/).

A practitioner's view

James Tumbridge

The greatest problem with regulators is the view they are always virtuous. Those who work at regulators are no better or worse than any other person, but that means there will always be less than perfect action because some of their staff will make errors. The trouble is the errors go uncorrected, and the accused suffer. Too often the press, the parliamentary select committees and the courts fail to hold regulators to account and fail to maintain a healthy sceptical scrutiny of their actions.

The second problem with regulators, and the ICO is a prime example, is the inequality of arms. They have the state behind them, so in effect limitless resources. It is expensive to obtain good advice and defeat a determined regulator who is using its position and resources to force a concession on a person who may not deserve punishment. The ICO is well aware it can be more costly to argue than to accept a fine.

To correct these two vices the regulators would need to be truly held to account. They would be bound by rules of candour and transparency so the accused can see clearly why the regulator is of the view they have done something wrong. The obligation would be to disclose all information gathered - good, bad and irrelevant - so the accused knows what they face.

The rules they operate by could include an obligation to help the accused know the case against them, and to remember they are innocent until proven guilty. The fact the regulator investigates and fines is a problem. There is insufficient oversight and review of those fines and those conclusions.

Cost control is another consideration. Whether it is the provision of legal aid or limits on recoverable costs, something could be done to ensure the accused can have justice and not be overawed by the regulator's spending power.

The last issue I would highlight on enforcement behaviours is that the ICO seems to have (or at least believes that it has) the power to compel the answering of an unlimited number of questions an unlimited number of times, a power which is not shared with other enforcement agencies. This relentless grind of answering questions, always on their timetable and without end, is another unfair tactic of the ICO. The ICO is not bound by the Police and Criminal Evidence Act (PACE) or the codes and this could be reviewed. Also, the fining powers are huge. In some cases, the level of the fine is greater than a corporate fine for manslaughter and yet the fining decisions are hopelessly weak and devoid of reasoning, let alone justice. The rationale for the size of fines is lacking. All too often the regulator assumes without evidence that a small number of complaints is proof that a large number of people were unhappy and fines are therefore higher than can be justified.

There are problems too that appeals give a false impression that the ICO's behaviour can be corrected - false because most cannot afford an appeal. The Eldon Insurance appeal decision[17] seems to have removed any doubt that unfairness by the ICO can be 'cured' by the tribunal on appeal, so the ICO really has few controls of fairness and procedure and is largely free to behave however it wants at the investigation and fining stages. This could be addressed. Reputational damage (and even real and immediate damage to share value for listed companies) to those who face

17 First-Tier Tribunal, General Regulatory Chamber, Information Rights, February 2020, Appeal Number EA/2019/0054-0059 (http://panopticonblog.com/wp-content/uploads/sites/2/2020/03/Leave.eu-Eldon-PECR-appeal.pdf).

even potential enforcement actions can be enormous. For example, BA and Marriott have been publicly chastised for supposedly egregious breaches, so far no fines have yet been formally issued.

Conclusion

While the ICO has been praised by business organisations for playing a valuable role in the development of data protection law and policy, particularly in international forums,[18] there is a strong argument that the Information Commissioner is overseeing a regime that is not meeting its objectives either in fundamental rights or economic terms. There is little evidence that the substantive objectives set out in either the Commission's or the UK's impact assessments are being met, or even measured. The 2019 Annual Governance Report by the International Association of Privacy Professionals found that fewer than half of respondents to its survey of privacy professionals consider that their organisation is fully or mainly compliant with the GDPR, yet investment in compliance activity has levelled off (IAPP 2019) (unsurprisingly, given the vast sums devoted to it in past years). The same report in 2018 found that 20 per cent of respondents admit that full GDPR compliance is 'truly impossible'. Given that the respondents to the IAPP survey are the most sophisticated and privacy conscious population, the chances of organisations across the wider economy being able to comply seem even more remote.

As the UK will no longer be bound by the precise requirements for supervisory authorities under the GDPR after the end of the Transition Period, the government will be able to introduce new requirements and controls on the Information Commissioner to improve accountability and improve the focus and quality of decision making within the ICO. The European Data Protection Board's Adequacy Referential (EDPB 2018) (which is guidance for the Commission in making its determination of

18 See, for example, the evidence of practitioners and industry bodies given to the House of Lords EU Committee in 2017 (https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/707.htm).

adequacy) requires, following the case law of the CJEU, that the third country's legal framework:

> must be '*essentially equivalent*' to that guaranteed in the EU, '*the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]*'. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.

The supervision and enforcement mechanisms form part of the core requirements and in particular the EDPB requires that a 'supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions'. Providing operational independence and impartiality are maintained, some reforms to the role and powers of the Information Commissioner should not adversely affect the UK's position as it seeks an adequacy decision. In fact, the reform options below are aimed at improving transparency and procedural fairness, in support of fundamental rights. Such steps will enable the UK to move towards the position favoured by the government at the inception of the GDPR, as outlined by the MoJ: 'a data protection framework that will stimulate economic growth and innovation, whist providing data subjects with a proportionate level of protection'.

Reforms could include:

- Reviewing the system of fines, to make sanctions more proportionate to harm, and reducing the cost of over-compliance identified by the MoJ.
- Reducing the scope of the tasks of the Commissioner by removing broader policy advisory matters to focus on the implementation and enforcement of the relevant laws and regulations.
- Allowing ministers to set policy guidance, which the Commissioner would be obliged to have regard to, similar to the way that, for example, energy and utility regulators Ofgem and Ofwat function under the Gas Act, Electricity Act and Water Industry Act respectively. This would strengthen democratic accountability.
- Increasing rigour in the scrutiny and accountability of the Information Commissioner by introducing a requirement to have measurable objectives (consistent with the requirements of relevant laws), set

by or in consultation with ministers, and transparently reported on to ministers and the DCMS Committee.

- Revising the appeal process and introducing procedural safeguards and cost capping, so that meritorious appeals are not discouraged by the burden of potential costs.
- Requiring the Commissioner to carry out impact assessments for future guidance that could have material economic effects (and suspending the coming into force of the AADCOP until an impact assessment, including a full cost benefit analysis and legal review, has been undertaken).

References

DCMS (2017) Data Protection Bill: summary assessment. London: Department for Digital, Culture, Media and Sport.

DCMS (2020) Explanatory memorandum to the Age Appropriate Design Code 2020. London: Department for Digital, Culture, Media and Sport.

European Commission (2012) Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Commission Staff Working Paper. Brussels.

European Commission (2020) Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. Brussels.

EDPB (2018) Adequacy Referential (originally produced by Article 29 Working Group). Revised and adopted on 6 February. Brussels: European Data Protection Board.

Godel, M., Landzaat, W. and Suter, J. (2017) Research and analysis to quantify the benefits arising from personal data rights under the GDPR. Report to the Department for Culture, Media and Sport. London: London Economics.

House of Commons and House of Lords Joint Committee on Human Rights (2020). Human Rights and the Government's Response to Covid-19: Digital Contact Tracing. Third Report of Session 2019–21. London: House of Commons.

IAPP (2019) IAPP-EY Annual Governance Report. Portsmouth, NH: International Association of Privacy Professionals.

Information Commissioner's Office (2019) Consultation on the Draft Framework Code of Practice for the Use of Personal Data in Political Campaigning, August. Wilmslow: ICO.

Information Commissioner's Office (2020) Age Appropriate Design: A Code of Practice for Online Services, January. Wilmslow: ICO.

Information Commissioner's Office (2020) Direct Marketing Code of Practice (draft), January. Wilmslow: ICO.

Information Commissioner's Office (2020) Letter from the Information Commissioner to Rt. Hon. Harriet Harman QC, MP, 11 May. Wilmslow: ICO.

Jia, J., Jin, G. Z. and Wagman, L. (2018) The Short-Run Effects of GDPR on Technology Venture Investment. NBER Working Paper No. 25248. Cambridge, MA: National Bureau of Economic Research.

Johnson, G. A. and Shriver, S. K. (2020) Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR. Working paper. (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686).

Ministry of Justice (2012) Proposal for an EU Data Protection Regulation. London: Ministry of Justice.

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41(1): 100-126.

The Institute of Economic Affairs
2 Lord North Street
London SW1P 3LB
Tel 020 7799 8900
email iea@iea.org.uk