Regulating the Information Society: Data Protection and Ireland's Internet Industry

Dr TJ McIntyre¹

UCD Sutherland School of Law

tjmcintyre@ucd.ie

This is the final accepted manuscript of a chapter to be published in David Farrell and Niamh Hardiman (eds), *The Oxford Handbook of Irish Politics* (Oxford: Oxford University Press, forthcoming 2020).

Introduction

Ireland has become a global hub for personal information with internet firms headquartered in Dublin collectively holding information on billions of users. But has Ireland been a responsible regulator of the way in which these firms use that data? In this chapter I examine the approach taken by the Irish state, tracing the evolution of data protection governance and its application to the internet industry.

I start by outlining the legal and policy context. I argue that regulation in this area has been hampered by a weak legislative framework and significant under-resourcing. Using Facebook as a case study, I examine how this has in turn prompted international pressure for stronger Irish regulation. I outline the government response to this pressure, and assess the impact of a new commitment to 'best in class' data protection regulation. I conclude by arguing that the state has yet to properly engage with the wider issues presented by its new role as a key jurisdiction for the internet industry, with data protection being just one of the aspects which needs more attention as Irish regulation increasingly has spillover effects into other jurisdictions.

Background

The growth of Ireland as an internet industry centre is well known. As Brazys and Regan note in their chapter in this volume, information technology firms have been a central part of the Irish government's foreign direct investment (FDI) strategy, encouraged by attractive tax policies. Starting with Google in 2003, successive US firms such as Facebook, Microsoft, PayPal, and LinkedIn have established headquarters for their EMEA or non-US operations in

---

¹ Disclosure: TJ McIntyre chairs the civil liberties group Digital Rights Ireland which campaigns on the issues discussed in this chapter.

Dublin (Newenham, 2015). Brexit has reinforced this trend by jeopardising the flow of personal data to the UK, putting data-intensive firms under pressure to relocate operations if they are to continue to serve the EU market (McCullagh, 2017). Ireland, favourably placed as an English-speaking common law jurisdiction, has benefitted as a result (Ram et al., 2018).

The international criticisms of Ireland are equally well known. From the late 1990s onwards, the state has been accused of harmful tax competition to bring in technology companies (Killian, 2006; Shaxson, 2015). More recently, especially following the Edward Snowden revelations of mass surveillance by the United States, these charges have been joined by the claim that it has failed to ensure adequate standards of data protection. For example, in 2013 German Chancellor Angela Merkel singled Ireland out for failing to protect German users, saying on national television that 'We have great data protection laws in Germany but if Facebook is based in Ireland, then Irish law applies' (Scully, 2013). In 2015 the prominent Green MEP, Jan Albrecht, tied these tax and privacy strands together when he explained Irish success in attracting internet firms as based on 'a neo-liberal dumping policy [which] created the most beneficial conditions for IT companies wishing to establish business operations in the country' (Albrecht, 2015). The suggestion is that Ireland uses regulatory competition across both tax and policy rules to compete for FDI (for discussion of regulatory arbitrage in general see e.g. Carruthers and Lamoreaux, 2016).

Ireland is not, of course, the only EU country in which data protection regulation has been patchy; while there has been little empirical work in this area, the studies which have been carried out agree that funding and enforcement strategies have been inadequate in many member states (Bamberger and Mulligan, 2013; Erdos, 2016; Custers et al., 2018). Nevertheless, the fact that so many internet firms are based in Dublin makes the Irish situation particularly significant.

Regulatory context

The governance of privacy in a broad sense encompasses a range of actors including state bodies, industry, and civil society as well as a range of instruments ranging from legislation to self-regulation to privacy enhancing technologies (Bennett and Raab, 2006). For the purpose of this chapter, however, I focus on the area of data protection and in this section I outline how data protection regulation developed in Ireland until the early 2010s when international criticism and a changing EU legal landscape forced a shift in government policy.

Legal framework

Irish data protection law has its origins in the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'). This was the first legally binding international instrument on the protection of personal data, and was the starting point for the later EU Data Protection Directive² (1995), which has since been replaced by the General Data Protection Regulation³ (GDPR) (2016). From Convention 108 onwards, these share two main goals: to facilitate 'the free movement of personal data' between countries, and to ensure a high level of protection for the 'fundamental rights and freedoms of natural persons and in particular [the] right to the protection of personal data'.⁴

These instruments have created a European model of data privacy which has proved influential worldwide, based on a comprehensive data protection law (not restricted to public bodies or particular industry sectors) setting out general principles regulating how data is collected and used, and enforced by an independent supervisory authority (Newman, 2012). Until the GDPR, however, this model still left huge room for national divergence. Convention 108 and the Data Protection Directive were not directly effective: they required domestic implementing legislation and gave states considerable discretion as to how they were to be applied. As a result, both the substantive and procedural rules varied considerably between EU member states.

The Irish implementing legislation (the Data Protection Acts 1988 and 2003) took a particularly narrow approach, establishing the Data Protection Commissioner (DPC) as a supervisory authority with wide investigative and enforcement powers but almost no punitive capability. The legislation constrained the DPC by imposing a statutory duty to seek an 'amicable resolution' of every complaint before proceeding to make a formal decision.⁵ Uniquely amongst EU states, the DPC was not given the power to impose administrative sanctions,

---

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

⁴ Article 1 GDPR.

⁵ Data Protection Acts 1988 and 2003, section 10(1)(b)(ii).

reflecting constitutional concerns with conferring such a power on an administrative agency (De Hert and Boulet, 2016). However the lack of administrative sanctions was not counterbalanced by corresponding criminal offences: even deliberate or reckless breaches of data protection law did not constitute a crime except in a very small number of situations such as private investigator 'blagging' of information (Data Protection Review Group, 2010). The result, considered in terms of the classic Ayres and Braithwaite model of responsive regulation (examined in more detail by Scott, this volume), was a significant gap at the top of the pyramid of sanctions which left the DPC with no escalation strategy to deal with particularly serious cases (Ayres and Braithwaite, 1992: ch. 2).

Resources

The problem of limited powers was exacerbated by resource constraints, particularly as the DPC's remit extends to all public and private sector organisations as well as the information technology sector. Established in 1989 with six staff, by 2001 the DPC still had only eight staff despite a significantly increased workload and successive annual reports describing 'completely inadequate staffing' (Data Protection Commissioner, 2002). 2002 saw the number of staff raised to 16 with a maximum complement set at 21, and numbers hovered around this level for the following decade. Despite this increase, the office was still under-resourced for the specialist issues presented by the internet giants beginning to locate in Dublin; remarkably, it did not have either an in-house lawyer or an in-house technical expert until 2012 (Data Protection Commissioner, 2014).

These issues were compounded by a 2003 government decision to relocate the agency from Dublin to Portarlington as part of a programme of decentralisation to promote rural development (for background on the ill-fated decentralisation scheme see Humphreys and O'Donnell, 2006). Portarlington, a town of 4,000 people about 80km from Dublin with few amenities, proved unattractive to the Dublin based staff: all but one declined to move when the transfer took place between 2005 and 2007. The result was an almost complete loss of expertise, and an organisation which had to be rebuilt largely from scratch – an unwelcome distraction which left the DPC playing catch up at a time when internet firms were increasing their activities in Dublin.

Apart from the disruption, the move to rural Ireland also inadvertently cemented the international perception of Ireland as an inadequate guardian of personal data. When the wider

decentralisation programme was eventually cancelled, plans for purpose-built accommodation were abandoned and the DPC's temporary offices above a convenience store became its long-term home. As international attention began to focus on Ireland, photographs of this unprepossessing accommodation became journalistic shorthand for the mismatch between the regulator and regulated. Marsden has dubbed this 'the Portarlinton effect' – a 'flag of convenience national regulator' providing 'inadequate oversight' of US multinationals (Marsden, 2018: 392–94).

Government policy

Considered in the context of wider government policy, this failure to provide an adequate regulatory system for data protection might appear surprising. From the mid-1990s onwards the government had targeted an Information Society strategy which achieved significant reform in areas such as copyright, electronic transactions, and digital signatures (Harney, 2002). Data protection was an obvious component of this strategy, and the Information Society Commission – an independent body set up to make policy recommendations to government – identified several areas where updated data protection laws were needed ('Building the Knowledge Society', 2002).

Despite this, data protection continued to lag behind. For example, the Data Protection Directive – identified by the Information Society Commission as a priority – should have been transposed into Irish law by 1998 but was not implemented in full until 2003. A 2010 report identifying a need for data breach rules was never progressed, leaving Ireland without any mandatory data breach notification until 2018 (Data Protection Review Group, 2010). The statutory power to give parliamentary approval to codes of conduct drawn up by the DPC was never used, meaning that those codes of conduct remained non-binding with no incentive to comply other than possible reputational harm. The overall picture during this time is one of minimal legislative activity, with such activity as there was prompted largely by the need to comply with EU obligations.

Why this inertia? A lack of regulatory capacity probably played a part. Data protection has been the responsibility of the Department of Justice and Equality – a body that has struggled with poor governance for many years. Following a political crisis in 2014 (which resulted in the sequential departures of the Garda Commissioner, the Minister, and the Secretary General of the Department – discussed further by Conway, this volume) an independent review

commissioned by the incoming Minister described the Department in damning terms as having 'significant leadership and management problems', with a 'closed, secretive, and silo-driven culture' and hampered by a sprawling remit making the Department 'quite unique in the breadth of [its] responsibilities' ('Report of the Independent Review Group on the Department of Justice and Equality', 2014). This may explain some of these failings: when the Department has been busy firefighting in other areas, it is not surprising that data protection has received less attention.

Lack of regulatory motivation, however, appears to have been the main factor. The Department of Justice and Equality is not a natural home for data protection regulation; it has historically given little weight to privacy rights, treating them as a hindrance to its core functions in relation to state security and law enforcement. For example, in the area of surveillance the Department has used a strategy of secrecy to avoid fundamental rights scrutiny by '[using] surveillance without any explicit legal basis, with regulation introduced reluctantly and belatedly when some scandal or outside pressure pushed the issue onto the agenda' (McIntyre, 2015a: 290). Indeed, a similar hostility to data protection has been endemic throughout much of the public sector – so much so that the former DPC, Billy Hawkes, said shortly before his retirement that 'audits of State organisations have, in too many cases, shown scant regard by senior management to their duty to safeguard the personal data entrusted to them... I have often felt I was fighting a losing battle in stressing the need for proportionality in this area' (Edwards 2014; Hawkes 2014).

At the EU level the Irish state has taken an equally restrictive approach to information privacy rights. Ireland opposed the adoption of the Data Protection Directive – arguing instead that Convention 108 was sufficient – and went on to resist many of the key aspects of the Directive such as the provisions for sensitive personal data and the requirements for notification of data processing (Bignami, 2005). Similarly, an analysis of leaked documents from the negotiation of the GDPR placed Ireland among the top three countries seeking to water down the draft regulation, with 33 of 34 amendments proposed by Ireland being described as weakening data protection rights ('Governments Rating', 2015; Scally, 2015a).

This institutional indifference to data protection went largely unchecked by any significant countervailing forces. Compared to other EU countries, until recently Ireland has had relatively little public concern or political debate regarding privacy issues (Custers et al., 2018). Civil

society involvement was also limited – unlike the UK or Germany, which each have several well-funded bodies focused on privacy rights, Irish advocacy in this area has mostly been carried out by the NGO Digital Rights Ireland which has a small annual budget and no paid staff (though the better resourced Irish Council for Civil Liberties has become more active in this field from 2016). There was little business pressure for data protection reform, and where changes were sought these were almost invariably in the direction of weakening individual rights rather than strengthening enforcement (see e.g. Legal Affairs Working Group, 2002).

Facebook and its fallout

Pressure for change in the Irish data protection landscape began to grow in the early part of the 2010s. There were a number of contributing factors, including the 2013 Snowden leaks, a growing public awareness of privacy issues generally, and the European Commission review of the operation of the Data Protection Directive, which identified a significant divergence in protection between member states (Commission of the European Communities, 2010). However, probably the single most significant element was the 2010 decision of Facebook to change its terms of use so that users outside the USA and Canada would be governed by a contract with Facebook Ireland Ltd. rather than Facebook Inc. in California.

Although Facebook first opened a Dublin office in 2008, the 2010 change was significant in that it brought its users outside North America clearly within the remit of the DPC. As the Data Protection Directive was then understood, this had the effect of putting regulation of Facebook's operations under Irish jurisdiction to the exclusion of other EU member states. The result was that users and regulators elsewhere in Europe became largely dependent on the DPC to take action on their concerns – giving the DPC significant extraterritorial reach while also exposing it to international scrutiny (Hijmans, 2016).

With Facebook established in Dublin, complaints to the DPC soon followed. The most important were brought by Max Schrems, an Austrian privacy activist, who filed 23 distinct complaints between August 2011 and July 2013 challenging a range of practices from facial recognition to tracking of non-users (Schrems, 2014). These attracted media interest throughout Europe and formed a central part of a DPC audit of Facebook's privacy practices in 2011 and a follow-up audit carried out in 2012 (Data Protection Commissioner 2011, 2012b).

It is no exaggeration to say that these complaints ultimately reshaped the European and trans-Atlantic privacy landscape. They prompted two sets of litigation (one still ongoing at the time of writing), two references by the Irish courts to the European Court of Justice, and a landmark decision from the Court of Justice invalidating the European Commission's Safe Harbour decision permitting the transfer of personal data to the United States. While the full detail of the Facebook investigation and subsequent litigation is beyond the scope of this chapter, a number of aspects can be picked out which illustrate the wider experience of data protection in Ireland.

Resources

The Facebook audits highlighted the resource constraints faced by the DPC; during the first audit the DPC was forced to rely for technical expertise on an academic expert acting *pro bono*, lacking any in-house capability (Data Protection Commissioner, 2011: 22–23). The first audit occupied a quarter of the DPC staff for three months, hindering their other work, and ruling out any similar investigation in relation to other multinational companies (Data Protection Commissioner, 2012a). The cost of legal fees in the subsequent Facebook litigation has also been significant. A full breakdown of fees is only available for 2016 and 2017, but in those two years the DPC has spent €1.9 million on legal fees and related litigation costs on this one matter – one-sixth of its total budget over that period (Deegan, 2018).

Regulatory strategy

One of the most controversial aspects of the Facebook investigation was the way in which the complaints were handled. The two audit reports were not formal decisions on the complaints made by Schrems. Instead the DPC characterised them as a form of cooperative engagement with Facebook, resulting in *recommendations* rather than *requirements*. This reflected a general preference of the DPC to avoid adversarial enforcement processes where possible, prioritising compliance through the use of soft enforcement tools (McGeveran, 2016).

There is nothing inherently undesirable about this approach, which in this case did result in a number of improvements in Facebook's privacy practices. Indeed the European data protection model envisages that the supervisory authorities will have a number of overlapping functions, and Bennett and Raab (2006) have described them as variously playing the roles of ombudsman, auditor, consultant, educator, negotiator, policy adviser, and enforcer. McGeveran (2016) has argued that the Facebook investigation should be seen as a successful

example of responsive regulation within the Ayres and Braithwaite (1992) model – not just in relation to the audits themselves but by fostering an ongoing cooperative relationship with the regulator.

Against that, however, the handling of the audits illustrates the problems with these informal processes. In 2014 Schrems eventually withdrew 22 of the 23 complaints as a result of his frustration with the approach taken by the DPC, which he characterised as avoiding formal decisions, failing to ensure procedural fairness by refusing him access to the submissions made by Facebook on the points he raised, conflating 'best practice' with legal requirements, and adopting interpretations of the law that were contrary to the consensus understanding of the Data Protection Directive adopted by other EU data protection authorities (Schrems, 2014). A central criticism was that by 2014, nearly three years after many of the complaints were first made, he still had not received any formal decision. He also noted a perverse effect of the DPC's duty to seek an amicable resolution, arguing that it unduly personalised systemic issues. As he put it, '[o]ur campaign is meant to test Facebook Ireland Ltd. against the rights of all users under European law and not against our personal luck in bargaining' (Schrems, 2012).

This preference for cooperative engagement over formal adjudication is not unique to the DPC; there is a well-known tendency amongst Irish regulators to prefer soft enforcement measures even where sanctions are available (Brown and Scott, 2010; Collins, 2010). It is understandable that the DPC would take this approach, given the statutory obligation to seek an amicable resolution, the under-resourcing of the office, and the extremely high cost of litigation in Ireland. Nevertheless, the Schrems complaints illustrate how informal engagement can compromise the role of the regulator to adjudicate on complaints that fundamental rights have been violated.

The remaining Schrems complaint also illustrates failings in the approach taken by the DPC, and in particular a tendency to take an excessively narrow, risk-averse view of the law. That complaint was filed after the Snowden revelations, and asked the DPC to take action to prohibit the transfer of his personal data from Facebook Ireland Ltd. to Facebook Inc. on the basis that US law did not provide adequate protection of that data, particularly against mass surveillance programmes. The DPC, however, took the view that he was precluded from investigating by the Commission Safe Harbour decision of 2000, which permitted data transfers to the US in certain circumstances, and therefore dismissed the complaint as 'frivolous and vexatious'.

Following a judicial review and preliminary reference, the European Court of Justice disagreed; in what was widely seen as a rebuke to the DPC, the court held that it was 'incumbent upon the national supervisory authority to examine the claim with all due diligence' and, if necessary, to bring legal proceedings itself to vindicate the rights of the individual.⁶

International criticism

The DPC's handling of the Facebook complaints was in many ways out of line with the views taken by other European data protection authorities. Regulators in France, Belgium, the Netherlands and Germany had significantly more privacy-protective interpretations of the Data Protection Directive on topics such as the Facebook real-name policy and tracking on other websites, found their attempts to enforce frustrated by Facebook's establishment in Ireland, and were publicly critical of the Irish approach to an extraordinary degree (Schweda 2016).

Some focused on the state as a whole, stating that the DPC had his hands tied by a lack of funding and narrow domestic legislation. For example, the Data Protection Commissioner for Lower Saxony, Joachim Wahlbrink, said that 'Billy Hawkes does his best, but why is he expected to take on a plane like Facebook with a catapult?' (Scully, 2014). Other regulators were more directly critical of the DPC himself: the Data Protection Commissioner for Schleswig-Holstein, Marit Hansen, told newspapers that '[t]he Irish authority took a position of blind trust' (Scully, 2015b). However the consensus view was probably that of the former German Federal Commissioner for Data Protection and Freedom of Information, Peter Schaar, who bluntly said that: 'Of course Facebook would go to a country with the lowest levels of data protection... It's natural they would choose Ireland' (Scott, 2015).

Strong regulation as a competitive advantage

These criticisms of the Irish track record on data protection – by other national regulators, no less – reverberated with a media which had been sensitised to privacy issues by the Snowden stories, and resulted in an unprecedented degree of international scrutiny; in a first for the Irish public appointments system, when Billy Hawkes was nearing the end of his term of office as DPC in 2014 the *New York Times* ran a detailed story on the competition to select his replacement (Scott 2014).

---

⁶ Judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

The publicity was damaging to the point where some Dublin-based technology firms were themselves expressing concern about the international perception of the Irish system. In a private 2014 meeting between the Minister for Finance and the CEO of Google Ireland, Google stressed that 'the strength of a country's competent authority for data privacy was now as important an issue for a country's competitive edge as their competent authority for taxation' (Department of Finance, 2014). Thus, the politics of data protection and FDI shifted: the relatively lax data protection regime which had initially attracted major firms into Ireland, now becoming a liability and source of competitive disadvantage.

Although the government initially attributed this criticism to jealousy at Ireland's economic success, it ultimately accepted that a stronger enforcement system was necessary (Brennan, 2015). In 2014 the government designated a Minister of State with special responsibility for data protection and gave a commitment that Ireland would be 'best in class' in data protection regulation, investigation and enforcement. The press release announcing the decision is unintentionally candid about government priorities: it doesn't mention privacy or fundamental rights at any point, instead referring to 'measures aimed at ensuring that Ireland's approach to data protection in the digital economy... [is] *a strong support to economic development and Foreign Direct Investment*' (Department of Justice and Equality, 2014; 'Press Release: Minister Murphy Sets out Data Protection Roadmap after Cabinet Decision', 2014). As is often the case in Ireland, economic considerations prevailed where civil liberties concerns had not.

The coincidence that Billy Hawkes reached retirement in 2014 meant that the task of developing a 'best in class' regulatory body fell to his successor, Helen Dixon.⁷ In this she benefitted from significantly increased funding: from €1.7 million in 2013 to €15.3 million in 2019. Staff numbers in turn increased from 30 in 2013 to a projected 165 by the end of 2019 (Data Protection Commission, 2019a). In a 2018 survey of data protection authorities across the EU, these increases place Ireland second from the top on a per capita basis in relation to both numbers of staff and overall budget; falling behind only Germany, where the division of data protection functions between the federal government and the states results in a significantly higher total spend (Custers et al., 2018).

---

⁷ It should be noted that while Ms. Dixon is the current Data Protection Commissioner, the supervisory authority as a whole was restructured by the Data Protection Act 2018 and is now known as the Data Protection Commission. For consistency, this will also be referred to as the DPC.

Nevertheless, these figures are still low in absolute terms, given the extent of the Irish role in relation to much of the internet industry, and a simple numerical comparison obscures significant ongoing resource problems. Staffing still falls below the 200 identified by the DPC as the minimum necessary to handle all the regulatory functions, work continues to be hampered by legacy IT systems, and the workforce is spread over several locations and lacks permanent office space in Dublin (Carswell, 2018; Duffy, 2019). Most recently, the funding allocated for 2020 has been increased by less than one third of the additional amount requested in the DPC's budget submission, and the DPC has stated that planned activities for 2020 will be curtailed as a result (Data Protection Commission, 2019b).

Impact of the GDPR

As we have seen, a key criticism of the Data Protection Directive was that it permitted significant discrepancies between national implementations, leading to inconsistent levels of protection across Europe. The GDPR responds to this by prescribing both the substantive and procedural law in much more detail – the best known example being that each data protection authority must be empowered to impose fines of up to €20 million or 4 per cent of annual global turnover, significantly enhancing the capabilities of the Irish regulator.

The GDPR also addresses concerns about forum shopping by multinational firms. In the original proposal for the GDPR the European Commission had proposed a strong 'One Stop Shop' mechanism, which would enable firms to streamline their dealings with regulators across the EU so that all their interactions would take place with the regulator in the country of their main establishment. However, following criticism that this would encourage firms to locate in lax jurisdictions, the final text now provides that the regulator in the country of the main establishment shall be the 'lead supervisory authority' but must cooperate with 'concerned supervisory authorities' – i.e. regulators from other member states who have an interest in a particular matter, for example where individuals in their countries have complained about a firm. The lead supervisory authority must endeavour to reach a consensus with the other concerned authorities about the handling of complaints; should they not be able to do so, the concerned authorities can have recourse to the newly created European Data Protection Board (EDPB) which can make binding decisions regarding the dispute. In cases of urgency, other supervisory authorities can also take unilateral measures independently of the lead authority,

provided that these measures are provisional (for no more than three months) and are limited to their own territories (see e.g. Davies, 2016).

This system was adopted at a time when the Irish handling of Facebook was prominent in the news, and directly reflects concerns about inadequate enforcement in a number of jurisdictions including Ireland and the UK (McCullagh, 2017). Along with other aspects of the GDPR – such as new obligations in relation to mutual assistance and joint operations between national regulators – it exemplifies what Lynskey (2017) has described as a 'Europeanisation' of data protection law in which the GDPR harmonises the substantive law, the procedural mechanisms for enforcement, and the regulatory approaches to be taken, limiting the scope for divergent national positions.

Conclusion

The dominant international narrative is one of Ireland as the winner of a race to the bottom, sacrificing privacy protection of the European public for national economic advantage. It might be unfair to characterise this as a deliberate policy choice; as Sir Humphrey Appleby noted, one should be careful not to 'call Civil Service delays "tactics"... That would be to mistake lethargy for strategy' (Lynn and Jay, 1989: 110). But, whatever the motive, the result was a weak regulatory framework which helped attract inward investment to Ireland, and which was allowed to remain in place until the point where it became a threat to further investment.

From 2014 onwards, however, there has been a significant shift. Judged by the metric of funding per capita, Ireland now has one of the better resourced supervisory authorities in Europe. This, of course, is not the whole story: the extraterritorial reach of the Irish regulator means that we must consider funding *per user* rather than limiting ourselves to the Irish population and we have also noted other ongoing resource problems. However when put together with the new powers created by the GDPR it means that the regulator has the potential to act more effectively.

Whether this potential will be realised is another matter. The GDPR came into effect on 25 May 2018 but as of January 2020 the DPC has yet to make a final decision on any significant complaint regarding the internet industry. The DPC has described these delays as due to the need to ensure that a new and relatively untested law is applied in a way which stands up to legal challenge, but the old complaints about Irish enforcement are resurfacing. For example,

in December 2019 the Hamburg Data Protection Commission stated that 'After nearly one and a half years we must concede that we have a huge problem with the enforcement of cross border processing... [it] is absolutely unsatisfactory to see that the biggest alleged data protection violations of the last 15 months with millions of individuals [concerned] are far away from being sanctioned' (Vinocur, 2019). Similarly, the German Federal Commissioner for Data Protection and Freedom of Information, Ulrich Kelber, has highlighted the fact that the DPC was refused the additional funding sought for 2020, describing this as causing 'misery' for the Irish regulator (Krempel, 2019).

It is too soon to say how Irish enforcement of the GDPR will play out. A series of major decisions in relation to internet firms are due in 2020 which may either address or reinforce international criticism. However it is clear that the regulatory dynamic has changed since the adoption of the GDPR. The new lead supervisory authority/concerned supervisory authority rules are extremely significant: data protection authorities who have been critical in the past are now in a position to challenge any backsliding on the part of the DCP. One can expect this to result in close scrutiny of the Irish approach to firms such as Facebook, though not necessarily in an adversarial way: the new GDPR provisions for mutual assistance and joint operations have the potential to allow for much greater cooperation between national regulators (Barnard-Wills et al., 2016) and it has been reported that the German Federal Commissioner for Data Protection and Freedom of Information has agreed to support the DPC with discrete aspects of cross-border investigations (Krempel, 2019).

Finally, we should note that despite these new regulatory powers and resources, there are wider issues around the protection of data in Ireland which are far from settled. Despite the long-standing commitment to an Information Society, there have been many areas where national law and practice has failed to keep up, particularly in relation to the policing of cybercrime. The failure to legislate for law enforcement access to data held in Ireland has been a particular grievance for other EU member states who see Irish practice as hindering criminal investigations (see e.g. McIntyre, 2015b; Commission of the European Communities, 2016). As the Schrems case illustrates, Ireland's role as a global data hub has also put it in the thick of an ongoing transatlantic debate about state surveillance (for background see e.g. Vermeulen and Lievens, 2017). Despite this, there has been almost no public engagement on these issues, which have remained confined within the 'culture of secrecy' in the Department of Justice and Equality. It may well be that it takes another high profile episode such as the Max Schrems

complaints, with corresponding international embarrassment and threat to FDI, to force action in these areas.

Bibliography

- Albrecht, Jan-Philipp (2015). *Hands off Our Data*. Brussels: Greens EFA.
<https://www.janalbrecht.eu/2015/10/2015-10-14-hands-off-our-data/>.
- Ayres, Ian, and John Braithwaite (1992). *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press.
- Bamberger, Kenneth A, and Deirdre K Mulligan (2013). 'Privacy in Europe: Initial Data on Governance Choices and Corporate Practices'. *George Washington Law Review* 81 (5): 1529.
- Barnard-Wills, David, Cristina Pauner Chulvi, and Paul De Hert (2016). 'Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU'. *Computer Law & Security Review* 32 (4): 587–98.
<https://doi.org/10.1016/j.clsr.2016.05.006>.
- Bennett, Colin J., and Charles D. Raab (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd ed. London: Routledge.
- Bignami, Francesca E. (2005). 'Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network'. *Michigan Journal of International Law* 26: 807–68.
- Brennan, Michael (2015). "'Jealousy" is why Germany is irate over Irish data protection laws'. *Sunday Business Post*, 17 January 2015. <https://www.businesspost.ie/more-business/jealousy-why-germany-is-irate-over-irish-data-protection-laws-5f9fd660>.
- Brown, Ciara, and Colin Scott (2010). 'Regulation in Ireland: History, Structure, Style and Reform'. UCD Geary Institute Discussion Paper 44.
<http://www.ucd.ie/geary/static/publications/workingpapers/gearywp201044.pdf>.
- 'Building the Knowledge Society' (2002). Dublin: Information Society Commission.
https://www.taoiseach.gov.ie/eng/Work_Of_The_Department/Information_Society_Commission/Information_Society_Commission/Building_the_Knowledge_Society_Report_to_Government.pdf.
- Carruthers, Bruce G., and Naomi R. Lamoreaux (2016). 'Regulatory Races: The Effects of Jurisdictional Competition on Regulatory Standards'. *Journal of Economic Literature* 54 (1): 52–97. <https://doi.org/10.1257/jel.54.1.52>.

- Carswell, Simon (2018). 'Fit for Purpose? Can the Data Regulator Handle GDPR?' *The Irish Times*, 25 May 2018. <https://www.irishtimes.com/business/technology/fit-for-purpose-can-the-data-regulator-handle-gdpr-1.3507144>.
- Collins, Neil (2010). 'Re-Imagining Regulation for Democratic Political Systems: Lessons from Ireland'. *Journal of Comparative Politics* 3 (1): 21.
- Commission of the European Communities (2010). 'A Comprehensive Approach on Personal Data Protection in the European Union'. COM(2010) 609 final.
- Commission of the European Communities (2016). 'Non-Paper'. December 2016. <http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf>.
- Custers, Bart, Francien Dechesne, Alan M. Sears, Tommaso Tani, and Simone van der Hof (2018). 'A Comparison of Data Protection Legislation and Policies across the EU'. *Computer Law & Security Review* 34 (2): 234–43. <https://doi.org/10.1016/j.clsr.2017.09.001>.
- Data Protection Commission (2019a). 'Annual Report 25 May - 31 December 2018'. Dublin. <https://www.dataprotection.ie/sites/default/files/uploads/2019-03/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf>.
- Data Protection Commission (2019b). 'Statement on increased funding of €1.6 million in 2020 Budget'. <https://www.dataprotection.ie/news-media/press-releases/data-protection-commission-statement-increased-funding-eu16-million-2020>.
- Data Protection Commissioner (2002). 'Annual Report 2001'. Dublin. https://www.dataprotection.ie/documents/annualreports/annual_report_2001.pdf.
- Data Protection Commissioner (2011). 'Facebook Ireland Report of Audit'. Portarlington. <https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf>.
- Data Protection Commissioner (2012a). 'Annual Report 2011'. Portarlington. <https://www.dataprotection.ie/documents/annualreports/AnnualReport2011.pdf>.
- Data Protection Commissioner (2012b). 'Facebook Ireland Ltd Report of Re-Audit'. Portarlington. https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.
- Data Protection Commissioner (2014). 'Annual Report 2013'. Portarlington. <https://www.dataprotection.ie/docimages/documents/Annual%20Report%202013.pdf>.

- Data Protection Review Group (2010). 'Report of the Data Protection Review Group'. Dublin.
<http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwithcover.pdf>.
- Davies, Simon (2016). 'The Data Protection Regulation: A Triumph of Pragmatism over Principle?' *European Data Protection Law Review* 2 (3): 290–96.
<https://doi.org/10.21552/EDPL/2016/3/5>.
- De Hert, Paul, and Gertjan Boulet (2016). 'The Co-Existence of Administrative and Criminal Law Approaches to Data Protection Wrongs'. In *Enforcing Privacy*, edited by David Wright and Paul De Hert, 441–54. Cham: Springer International Publishing.
- Deegan, Gordon (2018). 'Data Protection Chief's €2m Bill for Facebook Court Fight'. *Irish Independent*, 16 January 2018. <https://www.independent.ie/business/irish/data-protection-chiefs-2m-bill-for-facebook-court-fight-36490990.html>.
- Department of Finance (2014). 'Summary Note of Meeting with John Herlihy and Urs Hozle of Google'. 5 November 2014. <https://www.digitalrights.ie/dri/wp-content/uploads/2015/05/Note-of-meeting-between-Google-and-Noonan.pdf.pdf>.
- Department of Justice and Equality (2014). 'Press Release: Murphy Announces Doubling of Funding for Office of the Data Protection Commissioner'. 18 December 2014.
<http://www.justice.ie/en/JELR/Pages/PR14000373>.
- Duffy, Rónán (2019). 'Revealed: Data Protection Commission's pleas for more staff and “fit-for-purpose” office'. *TheJournal.ie*, 12 October 2019. <https://www.thejournal.ie/data-protection-budget-4848807-Oct2019/>.
- Edwards, Elaine (2014). 'Public Service Told to Better Protect Personal Data'. *The Irish Times*, 12 May 2014. <https://www.irishtimes.com/news/ireland/irish-news/public-service-told-to-better-protect-personal-data-1.1792062>.
- ErDOS, David (2016). 'European Data Protection Regulation and Online New Media: Mind the Enforcement Gap'. *Journal of Law & Society* 43 (4): 534–64.
<https://doi.org/10.1111/jols.12002>.
- 'Governments Rating' (2015). LobbyPlag.Eu. 2015. <http://lobbyplag.eu/governments>.
- Harney, Mary (2002). 'Vision and Leadership in the Digital Economy'. In *Delivering the Vision: Public Services for the Information Society and the Knowledge Economy*, edited by Eileen M Milner, 195. London: Routledge.
- Hawkes, Billy (2014). 'Data Protection – the State, Technology and Other Challenges'. Institute of International and European Affairs, July 21.

- http://www.iiea.com/event/Billy_Hawkes-IIEA_21_July_201443bf.pdf?urlKey=keynote-address-billy-hawkes.
- Hijmans, Hielke (2016). 'The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European'. *European Data Protection Law Review (EDPL)* 2: 362–72.
- Humphreys, Peter C., and Orla O'Donnell (2006). *Public Service Decentralisation: Governance Opportunities and Challenges*. CPMR Discussion Paper 33. Dublin: Institute of Public Administration.
- Killian, Sheila (2006). 'Where's the Harm in Tax Competition? Lessons from US Multinationals in Ireland'. *Critical Perspectives on Accounting* 17 (8): 1067.
- Kreml, Stefan (2019). 'Große DSGVO-Verfahren: Deutsche Datenschützer wollen die Iren zum Jagen tragen'. heise online, 27 November 2019.
<https://www.heise.de/newsticker/meldung/Grosse-DSGVO-Verfahren-Deutsche-Datenschuetzer-wollen-die-Iren-zum-Jagen-tragen-4597554.html>
- Legal Affairs Working Group (2002). 'Building Trust through the Legal Framework'. Dublin: Information Society Commission.
https://www.taoiseach.gov.ie/eng/Work_Of_The_Department/Information_Society_Commission/Information_Society_Commission/Building_Trust_through_the_Legal_Framework.pdf.
- Lynn, Jonathan, and Antony Jay (1989). *The Complete Yes Minister*. New Ed edition. London: BBC Books.
- Lynskey, Orla (2017). 'The "Europeanisation" of Data Protection Law'. *Cambridge Yearbook of European Legal Studies* 19 (December): 252–86.
<https://doi.org/10.1017/cel.2016.15>.
- Marsden, Chris (2018). 'Prosumer Law and Network Platform Regulation: The Long View Towards Creating OffData'. *Georgetown Law Technology Review* 2: 23.
- McCullagh, Karen (2017). 'Brexit: Potential Trade and Data Implications for Digital and "Fintech" Industries'. *International Data Privacy Law* 7 (1): 3–21.
<https://doi.org/10.1093/idpl/ipw025>.
- McGeveran, William (2016). 'Friending the Privacy Regulators'. *Arizona Law Review* 58: 68.
- McIntyre, T.J. (2015a). 'Implementing Information Privacy Rights in Ireland'. In *Implementing Human Rights in Ireland*, edited by Suzanne Egan. Dublin: Bloomsbury Academic.

- McIntyre, T. J. (2015b). 'Cybercrime in Ireland: Towards a Research Agenda'. In *Routledge Handbook of Irish Criminology*, edited by Deirdre Healy, Claire Hamilton, Yvonne Daly, and Michelle Butler. Abingdon, Oxon ; New York, NY: Routledge.
- Newenham, Pamela (ed.) (2015). *Silicon Docks: The Rise of Dublin as a Global Tech Hub*. Dublin: Liberties Press.
- Newman, Abraham L. (2012). 'The Governance Of Privacy'. In *The Oxford Handbook of Governance*, edited by David Levi-Faur. Oxford: Oxford University Press.
<http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199560530.001.0001/oxfordhb-9780199560530-e-42>.
- 'Press Release: Minister Murphy Sets out Data Protection Roadmap after Cabinet Decision' (2014). MerrionStreet.Ie. 7 October 2014. http://www.merrionstreet.ie/en/News-Room/Releases/Minister_Murphy_sets_out_Data_Protection_Roadmap_after_Cabinet_Decision.html.
- Ram, Aliya, Mehreen Khan, and Nicholas Megaw (2018). 'Companies Review Arrangements for Data Transfer after Brexit'. Financial Times. 11 August 2018.
<https://www.ft.com/content/858e615c-9a63-11e8-9702-5946bae86e6d>.
- 'Report of the Independent Review Group on the Department of Justice and Equality' (2014). Dublin. <http://www.merrionstreet.ie/en/wp-content/uploads/2014/07/final-report.pdf>.
- Scallan, Derek (2014). 'Ireland: Prisoner of Big Tech?' *The Irish Times*, 3 May 2014.
<http://www.irishtimes.com/news/technology/ireland-prisoner-of-big-tech-1.1781833>.
- Scallan, Derek (2015a). 'Ireland in Top Three EU Countries for Undermining Data Privacy'. *The Irish Times*. 10 March 2015.
<https://www.irishtimes.com/business/technology/ireland-in-top-three-eu-countries-for-undermining-data-privacy-1.2133393>.
- Scallan, Derek (2015b). 'Data Watchdog's "Blind Trust" Criticised by German Regulators'. *The Irish Times*, 5 October 2015.
<https://www.irishtimes.com/business/technology/data-watchdog-s-blind-trust-criticised-by-german-regulators-1.2378315>.
- Schrems, Max (2014). 'Legal Procedure against "Facebook Ireland Limited"'. Europe v. Facebook. 2014. <http://europe-v-facebook.org/EN/Complaints/complaints.html>.
- Schrems, Max (2012). Letter to Data Protection Commissioner. 2012. 'Recent Report on Facebook Ireland Ltd.', 2 January 2012. http://www.europe-v-facebook.org/ODPC_JAN_pub.pdf.

- Schweda, Sebastian (2016). 'Under Close Scrutiny: German Courts and Authorities Investigate Facebook's Compliance with National Data Protection Law Reports: Germany'. *European Data Protection Law Review* 2: 414–21.
- Scott, Mark (2014). 'Irish Panel to Pick a Regulator With Global Reach in Overseeing Data Privacy'. *The New York Times*, 28 August 2014.
<https://www.nytimes.com/2014/08/29/technology/irish-panel-to-pick-privacy-regulator-with-global-reach.html>.
- Scott, Mark (2015). 'Irish Regulator Says Country Will Stay at Center of Online Privacy Debate'. *The New York Times*, 23 June 2015.
<https://bits.blogs.nytimes.com/2015/06/23/irish-regulator-says-country-will-stay-at-center-of-online-privacy-debate/>.
- Shaxson, Nick (2015). 'Narrative Report on Ireland'. Chesham: Tax Justice Network.
<https://www.taxjustice.net/2015/11/11/how-ireland-became-an-offshore-financial-centre/>.
- Vermeulen, Gert, and Eva Lievens (2017). *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance, and Big Data*. Maklu.
<http://hdl.handle.net/1854/LU-8541059>.
- Vinocur, Nicholas. (2019). "'We have a huge problem": European tech regulator despairs over lack of enforcement'. *POLITICO*, 27 December 2019.
<https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605>.