What the WhatsApp case reveals about the EU's GDPR enforcement system

Seamus Allen

Introduction

On Thursday, 2 September 2021, WhatsApp was fined €225 million by Ireland's Data Protection Commission (DPC), in the second biggest fine ever imposed under the European Union's General Data Protection Regulation (GDPR). WhatsApp has stated that it will appeal the decision.

While the size of the fine is impressive, the decisions taken by regulators regarding the transparency to which European citizens are entitled under the GDPR are just as important and likely to have far-reaching implications for many corporations handling personal data.

This case is particularly notable after a year in which Ireland's DPC and the EU's "One Stop Shop" system of GDPR enforcement have received frequent criticism. The WhatsApp decision has been hailed by some as a demonstration that this system of GDPR enforcement can work effectively, if given the time to do so.

However, if the case is examined in greater depth, it arguably demonstrates weaknesses in the EU's system of GDPR enforcement. The case highlights the sluggish pace of the "One Stop Shop" mechanism and the profound differences between European regulators. Combined with the narrow focus of the DPC's investigation, the case indicates that there are significant problems with the EU's system of GDPR enforcement.

This brief will outline the background to the case and the findings of the DPC. It will seek to explore whether the decision heralds change in the ability of European citizens to meaningfully control their personal data.

Background Issues: Increasing Scrutiny of the GDPR Enforcement System

It is notable that the WhatsApp decision was announced amidst a period of increasing scrutiny and criticism for Ireland's DPC and for

the EU's "One Stop Shop" mechanism. Under the GDPR's "One Stop Shop" mechanism, the lead supervisory authority for international companies is the national data protection regulator of the EU country in which these companies have their EU headquarters. Thus, Ireland is effectively the lead EU data protection regulator of the world's largest digital technology companies, as many of these companies are headquartered in Ireland. In recent years, Ireland's DPC has received criticism across Europe, including from privacy activists and from the European data protection regulators of other EU countries.[1] Critics claim that the Irish DPC's processes and procedures are inefficient and ineffective, thus creating a holdup on GDPR cases across Europe.[2] For its part, the DPC has pointed to its constrained resources, the complexity of GDPR cases, and the bureaucracy of the One Stop Shop System as causes of delay in its decision-making. As of mid-2021, Ireland's DPC was the lead supervisory authority for 196 cross-border cases in the EU but had reached draft decisions in only four cases.[3] Prior to the WhatsApp decision, it had only ever imposed one cross-border fine. In light of this situation, the European Parliament passed a resolution calling upon the European Commission to take infringement proceedings against Ireland in May 2021, while in July Ireland's Joint Oireachtas Committee on Justice urged reform of Ireland's DPC on the grounds that "citizens' fundamental rights are in peril."

Issues: WhatsApp's GDPR Infringements

The DPC's case against WhatsApp was based on four separate infringements.

The first infringement touches upon one of the most interesting aspects of data protection today: the question of which processes can convert personal data into data that is deemed genuinely anonymised and depersonalised.

1. *Schrems criticises Irish data regulator after Facebook case breakthrough*, Derek Scally, https://www.irishtimes.com/business/technology/schrems-criticises-irish-data-regulator-after-facebook-case-breakthrough-1.4457728; *Irish approach to data protection 'Kafkaesque', says Schrems*, Derek Scally, https://www.irishtimes.com/business/technology/irish-approach-to-data-protection-kafkaesque-says-schrems-1.4533257; *Max Schrems: Irish Data Protection Commissioner's process is designed to fail*, Cianan Brennan, https://www.irishexaminer.com/opinion/commentanalysis/arid-40252766.html; *German anger at Helen Dixon's defence of Ireland's record on tech multinational investigations*, Adrian Weckler, https://www.independent.ie/business/german-anger-at-helen-dixons-defence-of-irelands-record-on-tech-multinational-investigations-39020118.html; *Fight breaks out between Ireland and Germany over Big Tech regulation*, Financial Times, https://www.ft.com/content/37705bcf-c5b6-4ef0-adb8-35a8680dbaec; *Houses of the Oireachtas Joint Committee on Justice Report on meeting on 27th April 2021 on the topic of GDPR*, 2021-07-22_report-on-meeting-on-27th-april-2021-on-the-topic-of-gdpr_en.pdf (oireachtas.ie), p. 37-38

2. *DPC rejects criticism of its regulation of big tech companies*, Charlie Taylor, *Irish Times*, https://www.irishtimes.com/business/technology/dpc-rejects-criticism-of-its-regulation-of-big-tech-companies-1.4549370?mode=sample&auth-failed=1&pw-origin=https%3A%2F%2Fwww.irishtimes.com%2Fbusiness%2Ftechnology%2Fdpc-rejects-criticism-of-its-regulation-of-big-tech-companies-1.4549370; *MEPs call for infringement procedure against Ireland*, Luca Bertuzzi, *Euractiv*, https://www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/

3. *Data watchdog close to decisions on fines in up to seven 'Big Tech' investigations*, Simon Carswell, *Irish Times*, https://www.irishtimes.com/business/data-watchdog-close-to-decisions-on-fines-in-up-to-seven-big-tech-investigations-1.4494270; *Why is Ireland's Data Protection Commission under fire?*, Jenny Darmody, *Silicon Republic*, https://www.siliconrepublic.com/enterprise/dpc-data-protection-gdpr-helen-dixon; *Houses of the Oireachtas Joint Committee on Justice Report on meeting on 27th April 2021 on the topic of GDPR*, 2021-07-22_report-on-meeting-on-27th-april-2021-on-the-topic-of-gdpr_en.pdf (oireachtas.ie), p. 7

WhatsApp accessed the mobile phone numbers of non-users via the contacts lists of those who joined. Although it converted such mobile numbers into a new numerical value using an encryption process called 'lossy hashing' the European Data Protection Board determined that the new numerical value still constituted the personal data of non-WhatsApp users. Thus, the WhatsApp case arguably sets a high bar for processes that are intended to anonymise personal data. On this issue, WhatsApp was judged to have violated the GDPR due to a lack of transparency for non-users regarding its processing of their personal data, both before and after the lossy hashing process. This judgement may have implications for many other apps that access users' mobile phone contacts lists, and for many companies that use processes that are intended to anonymise personal data.

The next three issues relate to the transparency of information that WhatsApp provided regarding: (i.) its processing of users' personal data, (ii.) the personal data that WhatsApp shares with Facebook and (iii.) WhatsApp's compliance with the GDPR's general principles on transparency. A central theme of the DPC's findings was that the information provided by WhatsApp was often "vague, unclear and ambiguous". Users could only gather information on how their data was processed by searching across multiple documents and webpages. The DPC found that the unfriendly format potentially risked dissuading users from reading the policies and that WhatsApp had provided "meaningless and generalised information", as well as "misleading information" meaning that the reading process was a "needlessly frustrating exercise."

Again, these issues identified by the DPC are likely to have a far broader application right across the data economy. Many consumers will be aware of the frustration of reading corporate privacy policies. Indeed, one of WhatsApp's objections was precisely that its policy "aligns with the approaches adopted by industry peers" and "industry norms." This point is arguably correct - and therefore the DPC's decision may have broad-reaching implications for how companies write their privacy policies and public communications. The findings regarding WhatsApp's data sharing with Facebook was arguably the most severe breach of users' trust, with users being provided with "contradictory" information. Ultimately, the DPC described WhatsApp's four GDPR infringements as "very serious" and "severe in gravity."

Implications for the One Stop Shop

Despite the strong language of the draft decision, other European regulators believed that Ireland's DPC did not go far enough. When the provisional draft of Commissioner Dixon's decision was provided in December 2020, the national data protection regulators from seven other EU countries formally objected. These regulators argued that on the same themes of transparency investigated, multiple other GDPR transparency provision breaches had occurred in addition to those considered in the draft decision. After a failure to reach an agreement, the dispute was referred to the European Data Protection Board (EDPB) (which mainly consists of the national data protection authorities of the EU Member States) in April 2021. In July 2021 the EDPB found in favour of multiple objections, thereby forcing a revision of the Commissioner's provisional draft to include additional identified breaches of the GDPR.

The most striking disagreement, however, was regarding the size of the fine proposed. Commissioner Dixon initially proposed a maximum fine of €50 million – but was obliged

to increase this to €225 million by the EPDB. Commissioner Dixon believed that the four infringements were closely related and involved the same set of processing operations. Therefore, her view was that WhatsApp should be fined for the most serious infringement. The EPDB disagreed – it argued that there were four distinct infringements and that WhatsApp should be fined for each of these four GDPR violations. It argued that fining a company for only the most serious GDPR violation would allow a company to engage in multiple GDPR violations without facing extra penalties. Ultimately, it is clear that profound disagreements exist between Europe's data protection regulators regarding GDPR interpretation and enforcement.

On previous occasions when her office has been criticised, Commissioner Dixon explained that the pace of cross-border cases is often slowed by the complexities of the One Stop Shop system of co-decision making and the time required to resolve disagreements between regulators. The WhatsApp case would seem an apt demonstration of this. Commissioner Dixon first presented her draft decision to the other regulators in December 2020 and the resulting disagreements were not resolved until July 2021, more than half a year later. Commissioner Dixon has also stated that these cases are already time consuming due to the complexity of GDPR and the need to build tight cases that can hold up in court. Indeed, the WhatsApp investigation itself began in 2018. If Europe's data protection regulators could pool resources synergistically, it might be possible that cases could be advanced at a faster rate, with the additional manpower allowing for room to address complexity and build robust legal cases. Profound differences over GDPR interpretation might also be resolved at a much earlier stage in the enforcement process. At the heart of these issues is whether the burden of upholding the data rights of more than 400 million European citizens is appropriate for a small country depending only on its own resources.

Implications of a Narrow Transparency Case

However, it is the narrow scope of the WhatsApp investigation, considered alongside the problems of the One Stop Shop system, that most clearly illuminates the weaknesses of the EU's current GDPR enforcement system. The limited scope of the case combined with its prolonged duration may limit the impact of the WhatsApp decision for promoting citizens' data rights.

It should first be noted that the DPC's investigation was explicitly and exclusively "limited to an assessment of the extent to which WhatsApp complies with its transparency obligations pursuant to the GDPR." The official decision stated that other considerations "fall outside of the scope of this inquiry." Some issues touched upon naturally go beyond the requirements of transparency. For example, in her report, Commissioner Dixon suggests that WhatsApp's transparency breaches were sufficiently severe as to call into question whether users could exercise genuine "free will" and "autonomy" in their decisions. It could thus be queried, for example, whether WhatsApp's data transfers to Facebook are legal, given that they may be happening without the meaningful or informed consent of users.

Secondly, even as a transparency case, the DPC investigation was narrow in scope. The DPC almost exclusively relied on the publicly available policy documents and public communications provided by WhatsApp and assessed whether these were adequate compared to the general prescriptions of the GDPR regarding what such documents should

look like. The DPC did not generally examine what personal data WhatsApp processes and what it does with such data, in order to systematically compare this to what a reader can learn from WhatsApp's publicly available documents. Instead, the focus was on whether readers could obtain the information to which they were legally entitled by reading WhatsApp's publicly available documents. Commissioner Dixon repeatedly noted that she was unable to ascertain what WhatsApp did with users' personal data on the basis of such documentation. Without a comparison of such documents with what WhatsApp does with its users' data, the degree of WhatsApp's lack of transparency might not be adequately measured.

As a transparency case, and on its own merits, the WhatsApp case would have been a sign that the system was working well if it had been completed in 2018. But with the investigation beginning in 2018, the slow pace combined with the narrow scope of the investigation significantly detracts from the effectiveness of the result, for three reasons.

Firstly, whether or not the case improves transparency remains to be seen. While some corporations might scramble to rewrite their privacy policies, whether they do so in a way that provides meaningful transparency is far from assured. Some corporations may be tempted to take on board the specific items raised in the WhatsApp case while obscuring information in other ways – for example by spamming readers with exhaustively trivial information on every aspect of data processing. Given that it could be years before any action is taken against them, such practices might be judged by some companies as not being excessively risky.

Second, even if the WhatsApp decision helped to herald a new era of transparency, it arguably comes years too late to meaningfully empower users in many cases. Platforms such as WhatsApp that become socially embedded in society can become something upon which users can be dependent – for work group chats, family group chats, voluntary clubs and so on. A potential user who may have rejected installing WhatsApp had they been provided with genuine transparency several years ago may not feel they are in a position to reject WhatsApp today, due to the various social dynamics and pressures involved. Transparency that comes years late may do little to empower citizens to make genuinely autonomous choices.

Third, it is not clear that the case establishes a sufficient deterrent for other companies, some of whom might feel tempted to infringe the GDPR in the short-term, in order to establish positions of dominance. For example, a new company could seek to mislead users about its privacy standards, to gain trust and widespread use, calculating that it might have little to fear from a GDPR fine and transparency change that will affect it only several years later. By this time it may have become a platform on which users have become dependent and from which it is difficult to switch, due to social dynamics and pressures.

Conclusion

The DPC's case against WhatsApp illustrates some of the structural weaknesses of the EU's system of GDPR enforcement. Even a very narrowly scoped investigation into WhatsApp took two years to complete before it was then referred to the DPC's European colleagues, a majority of whom then significantly disagreed with aspects of the decision, thus prolonging the case further. The longer the duration of cases, the longer the infringements of citizens' rights can continue, and the more difficult it can be for citizens to meaningfully exercise their rights or to benefit once a case has finally been completed. As matters currently stand,

the national data protection regulators of different EU Member States are expending their resources in a manner that prolongs cross-border GDPR cases rather than expedites them. If EU regulators could strategically coordinate and pool resources, the opposite might be the case. This would likely require significant reform of the One Stop Shop mechanism however. Ultimately, the WhatsApp decision may lead to significant changes in how companies present information to their users. However, it seems less likely to meaningfully empower citizens' rights and seems to demonstrate that the EU's system of GDPR enforcement is not working as effectively as it should be.

The Institute of International and European Affairs (IIEA) is Ireland's leading international affairs think tank. Founded in 1991, its mission is to foster and shape political, policy and public discourse in order to broaden awareness of international and European issues in Ireland and contribute to more informed strategic decisions by political, business and civil society leaders.

The IIEA is independent of government and all political parties and is a not-for profit organisation with charitable status. In January 2021, the Global Go To Think Tank Index ranked the IIEA as Ireland's top think tank.

The IIEA acknowledges the support of the Europe for Citizens Programme of the European Union

IIEA
iiea.com
Sharing Ideas
Shaping Policy

The Institute of International and European Affairs,

8 North Great Georges Street, Dublin 1, Ireland

T: +353-1-8746756 F: +353-1-8786880

E: reception@iiea.com W: www. iiea.com