

Mr Alan Raine
Committee Secretary
Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

28 February 2023

**Submission to the inquiry on
the influence of international digital platforms**

Dear Mr Raine,

1. I write on behalf of the Irish Council for Civil Liberties (ICCL), Ireland's oldest non-profit human rights monitoring organisation. Our digital unit investigates, advocates, and litigates to enforce everyone's digital rights across Europe and beyond.
2. Previously, I served in senior executive roles in news publishing, online advertising, and technology industries, and have published two books on related matters. I have testified on these issues at the U.S. Senate, the European Union institutions, and the International Grand Chamber on Disinformation and Fake News.
3. We write in response to item E of the Inquiry's terms of reference: **the adequacy and effectiveness of recent attempts, in Australia and internationally, to regulate the activities of such international digital platforms.**
4. Three pieces of European legislation are particularly significant for international digital platforms: the General Data Protection Regulation (GDPR),¹ the new Digital Services Act,² and the new Digital Markets Act.³ European experience under the GDPR is likely to be of particular relevance.

Digital platforms and the EU General Data Protection Directive

5. The GDPR was applied in 2018 after a two year grace period. Both it and the earlier law it replaced were based on principles conceived in the United States in the early 1970s: the Fair Information Processing Principles.⁴
6. The GDPR reinforced the EU's existing data protection regime by empowering national supervisory authorities with formidable new investigative and sanctioning powers. These powers include the ability to raid organisations and compel information, to impose significant fines, and most importantly to block data use, which is the ultimate sanction for international digital platforms.⁵

7. Diligent use of these powers to supervise international digital platforms should have four significant benefits:

- a. **Hate & hysteria:** enforcement of GDPR Article 5, 6 and 9 would give people control over the toxic algorithms that insert hateful and divisive material in their video and social feeds. This is essential because stopping platforms' toxic recommender systems is far more effective than removing harmful content, and does not affect freedom of expression.
- b. **Control:** enforcement of GDPR Article 5(1)b and 6 would empower people to decide which parts of what platforms to reward with their data.
- c. **Competition and innovation:** enforcement of Article 5(1)b would deprive large platforms of their unlawful data advantage. They would no longer be able to automatically take data from one part of their business to prop up other parts. This would prevent digital platforms from cascading their monopolies from market to market. As a result, nascent competitors could compete and innovate, and rapacious data collection would no longer be the default digital business model.

In addition, enforcement of GDPR Article 30 obligations would revolutionise merger analysis. Companies are required to have an internal accounting of everything they do with personal data. This accounting should enable competition authorities to conduct a far more sophisticated analysis of the consequences of the merger, based on a forensic understanding of everything that both companies do with personal data.

- d. **Sustainable media:** enforcement of Article 5(1)b, c, e, and f would stop platforms from stealing publishers' audiences and monetising them at higher margin on their own properties.

Enforcement failure: reasons

8. Substantive enforcement has not materialised. This is evident from continuing infringement of the law by digital platforms, and by the wider tracking industry. We believe the primary causes of enforcement failure may be:

- i. Supervisory authorities lack a culture of aggressive investigation. Many authorities were setup under the 1995 EU Data Protection Directive, which most EU Member States transposed in to national law without providing for enforcement powers. As a result, many authorities were relegated in to an ineffectual compliance theatre rather than building investigative capacity and appetite.
- ii. The GDPR's "country of origin" principle makes the country where a company bases its European headquarters the lead supervisory authority for that company. No other supervisory authorities can intervene if the lead authority asserts this role. Four of the world's five biggest digital platforms (by market cap) are based in Ireland. The other, Amazon, is in Luxembourg. Inaction by Irish and Luxembourgish supervisory authorities has paralysed enforcement across the entire EU.

The animosity between the Irish authority and its counterparts was recently manifest when the Irish Data Protection Commission began legal action against all of other EU supervisory authorities (collectively, the European Data Protection Board) at Europe's highest court.⁶

- iii. The GDPR neglected to provide deadlines and strict requirements governing how lead authorities must cooperate with other authorities. This has allowed lead authorities to frustrate their peers. However, the European Commission will propose supplementary legislation to remedy aspects of this problem this year.⁷
 - iv. The European Commission has failed to perform its duty to monitor the application of EU Law by Member States, and to sue them when they fail to properly apply EU Law. This may soon be remedied: in January we secured a commitment from the European Commission to begin to monitor the progress of every significant GDPR investigation.⁸
9. Though investment in investigative, technical, and procedural law expertise appears to be inadequate, we do not believe that finance is the primary cause of the enforcement problem. The combined budget of European Economic Area supervisory authorities doubled from €167 million in 2016 to €338 million (\$532 million AUD) in 2022.⁹

Results of enforcement failure

10. Failure to enforce the GDPR against the primary offenders leaves small and medium enterprises in terror of GDPR enforcement. Rather than an instrument that protects people, the law is viewed as a nuisance.
11. Moreover, Europeans have been spammed every day for five years on 80%¹⁰ of the internet by unlawful "consent" popups. Though we eventually prevailed upon supervisory authorities to rule against this consent spam,¹¹ the tracking industry is now introducing variants of this same nuisance consent system globally.¹²

Right of private action

12. Despite the failure of supervisory authorities, Article 79 of the GDPR allows individuals to vindicate their rights at court. There is significant litigation underway as a result. However, this has a limited impact. Individuals can only litigate to vindicate their rights (Chapter 3 of the GDPR). They cannot litigate to enforce the obligations of digital platforms (Chapters 4 – 5). Only supervisory authorities can do so. In addition, whereas remedies imposed by supervisory authorities can apply across Europe, a litigant cannot achieve the same outcome as directly.

Digital Services Act and Digital Markets Act

13. The new Digital Services Act (DSA) will be enforceable on large digital platforms from February 2024. It contains two particularly important provisions that we believe are critically important to reduce online hate & hysteria.
- a. First, Article 38 compels digital platforms to give people the option to switch off the toxic algorithms that show them personalised material based on their political or

philosophical views, or ethnicity or other intimate characteristics. These recommender systems cause hate and division, for the reasons set out at paragraph 7 (a), above. The option to switch off a recommender system must be available whenever these algorithm are active.

- b. Second, Article 34 and 35 of the DSA require large digital platforms to assess and mitigate the risks caused by their systems, including risks to civic discourse and public security.¹³ This may be effective if we can avoid the platforms turning it in to compliance theatre.

14. The new Digital Markets Act (DMA) will be enforceable from March 2024. It prohibits large platforms (if designated as market “gatekeepers”)¹⁴ from combining and reusing their data in several ways:

- DMA Article 5(2)(a), requires that a platform refrain from using personal data collected through other companies that use its services;
- DMA Article 5(2)(b) and (c) and (d), prohibit platforms from automatically combining and cross-using personal data from different "core platform services" in their businesses;
- DMA Article 6(2), prohibits platforms from advantaging themselves by using data provided by businesses that use their services;
- DMA Article 6(9), requires that platforms give users the ability to take their data from its systems in order to use the data elsewhere; and
- DMA Article 6(10), requires that platforms provide access to business customers to the data they processes on those businesses behalf.

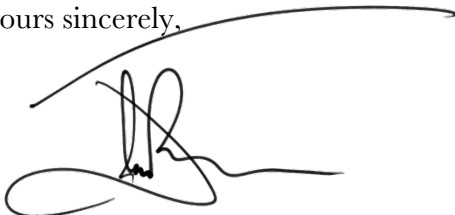
15. We anticipate that large digital platforms will be unable to comply with these DMA provisions, since they are unable to comply with analogous provisions under the GDPR, too.¹⁵

Conclusion

16. We believe that a well enforced GDPR-like law will be adequate and effective to regulate international digital platforms. The added measures in the DSA and DMA may be useful, but not essential if a GDPR-like law is robustly enforced.

17. We are at Committee Members’ disposal to assist them in their deliberations on these matters.

Yours sincerely,

A handwritten signature in black ink, appearing to be 'Johnny Ryan', with a long horizontal flourish extending to the right.

Dr. Johnny Ryan FRHistS
Senior Fellow

-
- ¹ 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.
- ² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.
- ³ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.
- ⁴ U.S. Department of Health, Education, and Welfare Advisory Committee, "Records, Computers and the Rights of Citizens," 1973 (URL: <https://ia801507.us.archive.org/11/items/1973-hew-report/1973-hew-report.pdf>).
- ⁵ The power to raid organisations is provided for in Article 58(1)(f), the power to compel information is provided for in Article 58(1)(a) and (e). The power to block data use is provided for in Article 58(2)(d) and (f) and (g).
- ⁶ Data Protection Commission v European Data Protection Board Case T-70/23 and Data Protection Commission v European Data Protection Board Case T-84/23.
- ⁷ "Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation", European Commission, 24 February 2023 (URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en).
- ⁸ "Europe-wide overhaul of GDPR monitoring triggered by ICCL", ICCL, 31 January 2023 (URL: <https://www.iccl.ie/digital-data/europe-wide-overhaul-of-gdpr-monitoring-triggered-by-iccl/>).
- ⁹ ICCL obtained budget information for each national and German regional supervisory authority from 2016 to 2022 from national and state budgets, or directly from the authority itself, or in their annual reports. Income from fines that is returned to the national treasurer was not counted.
- ¹⁰ See "IAB & IAB Tech Lab Respond with Support for OpenRTB and IAB Europe's Transparency & Consent Framework", IAB, 19 October 2020 (URL: <https://www.iab.com/news/iab-iab-tech-lab-respond-with-support-for-openrtb-and-iab-europe-transparency-consent-framework/>).
- ¹¹ "GDPR enforcers rule that IAB Europe's consent popups are unlawful", ICCL, 2 February 2022 (URL: <https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/>).
- ¹² Called the "Global Privacy Platform". See "IAB Tech Lab Finalizes Global Privacy Platform and Advises the Industry to Prepare for Updated US State-Level Signaling", IAB TechLab, 28 September 2022 <https://iabtechlab.com/blog/iab-tech-lab-finalizes-global-privacy-platform/>; and "Global Privacy Platform", IAB TechLab (URL: <https://iabtechlab.com/gpp/>).
- ¹³ Digital Services Act, Article 24(1)b.
- ¹⁴ DMA, Article 3.
- ¹⁵ See "Unsealed court documents reveal data anarchy at Meta", ICCL, 17 November 2022 (URL: <https://www.iccl.ie/news/unsealed-court-documents-reveal-data-anarchy-at-meta/>).