

Please cite as Guido Noto La Diega, 'Ending Smart Data Enclosures: The European Approach to the Regulation of the Internet of Things between Access and Intellectual Property', in Stacy-Ann Elvy and Nancy Kim (eds), *The Cambridge Handbook on Emerging Issues at the Intersection of Commercial Law and Technology* (Cambridge University Press 2023)

Ending Smart Data Enclosures: The European Approach to the Regulation of the Internet of Things between Access and Intellectual Property

[Guido NOTO LA DIEGA](#)*

«Freedom does not consist in any dreamt-of independence from natural laws, but in the knowledge of these laws, and in the possibility this gives of systematically making them work towards definite ends»
Engels, *Anti-Dühring* (1877)

1. Introduction: the problem of smart data enclosures and the necessity to open up the IoT

In January 2022, the European Commission published the outcome of its inquiry into the competition issues in consumer-facing Internet of Things (IoT)¹. A key concern that emerged was that the leading players in the IoT market amass huge amounts of data about the users of smart devices (hereinafter 'Things'),² enclose them, and prevent third parties from accessing them³. These smart data enclosures exist at the expenses of both consumers and competitors as they are at the root of unfair exclusivity and tying practices, limited interoperability, as well as the extension of dominant positions to adjacent markets⁴. Smart data enclosures harm society more widely, as they hamper the potential of the wealth of data generated by and through Things to address societal challenges (e.g. climate change, public health, etc.).⁵ While it is

* Associate Professor of Intellectual Property and Privacy Law, University of Stirling, UK; Martin-Flynn Global Law Professor, University of Connecticut, US; Coordinator, Scottish Law and Innovation Network (SCOTLIN), Scotland; Expert Group on AI and Data in Education and Training, European Commission, Belgium; Fellow, Nexa Center for Internet & Society, Italy. Many of the ideas put forward in this chapter come from conversations with colleagues; I am particularly grateful to Caroline B Ncube and Abbe Brown for generously sharing their thoughts on data, IP, and societal challenges at the SCOTLIN (En)lightening Talk "Clashing Forms of Regulation and Rights" (Friday 2nd December 2022). All views and errors are my sole responsibility.

¹ European Commission, 'Final Report - Sector Inquiry into Consumer Internet of Things' (2022) COM(2022) 19 final; European Commission, 'Staff Working Document SWD(2022) 10 Final' (2022). The focus was mostly on virtual assistants.

² The use of 'smart' in this paper comes with two caveats. First, 'smart' is increasingly referred to non-IoT entities, such as smart contracts. I intend to limit it to 'Things' and IoT systems. Second, 'smartness' is a typically human feature and the argument can be put forward that the anthropomorphising of technologies brings more confusion than clarity. Conversely, for me Things are smart in the more limited sense of being connected to the Internet, equipped with sensors and actuators, and capable of at least partly automated machine-to-machine communication. A number of different uses of 'smart' can be found in Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Elgar 2015) 22. For a critique of smartness see, e.g., Kieron O'Hara, 'Smart Contracts - Dumb Idea' (2017) 21 IEEE Internet Computing 97. On the issues of anthropomorphism and anthropocentrism in the IoT see Teodor Mitew, 'Do Objects Dream of an Internet of Things?' (2014) 23 Fibreculture Journal 1. For a definition of 'Thing', please see Guido Noto La Diega, *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies* (Routledge 2022) ch 1.

³ European Commission, 'Final Report - Sector Inquiry into Consumer Internet of Things' (n 2) esp. points 36 and 43.

⁴ The European Commission identifies these issues but depicts them as if they were discrete. I would posit that they are intimately intertwined and that data enclosures are at the centre of them all.

⁵ This was the focus of Guido Noto La Diega and Estelle Derclaye, 'Opening Up Big Data for Sustainability: What Role for Database Rights in the Fourth Industrial Revolution?' in Ole-Andreas Rognstad, Taina Pihlajarinne and Jukka Mähönen (eds), *Promoting Sustainable Innovation and the Circular Economy: Legal and Economic Aspects* (Routledge 2022).

usually recognised that data as such is not the subject of property rights,⁶ IoT companies can rely on trade secrets, database rights, technological measures, and contractual measures to exercise property-like powers over data.⁷ This monopolistic approach to data should be understood in the context of these companies' strategic use of terms and conditions, technical requirements and certification processes as tools to impose their '*proprietary technologies* [as] *de facto standards*.'⁸ More generally, it has been shown that ubiquitous computing leads to ubiquitous intellectual property (IP), as every layer of a Thing is covered by multiple overlapping IP rights (IPRs).⁹ Against this backdrop, it becomes easy to comprehend why the EU's data strategy focuses on improving access to data through a cross-sectoral data governance framework.¹⁰ While on the face of it these recent EU data governance laws go in the direction of more open, accessible, and re-usable data, they tend to balance that ethos with provisions that IoT big tech can use to retain and strengthen data enclosures. This chapter aims to critically assess whether the attempt to balance openness and IP results in the prevalence of closed IoT systems, thus ultimately preventing smart data from being re-used for the common good.

After becoming a global leader in the field of digital regulation with the General Data Protection Regulation (GDPR) – which prompted similar laws across the globe, from California through Turkey to China¹¹ – the European Union (EU) is at it again with the Artificial Intelligence (AI) Act.¹² The latter will ban certain practices (e.g. face recognition for law enforcement purposes)¹³ and impose human oversight, transparency, and other requirements on providers of high-risk AI systems (e.g. automated systems used in recruitment)¹⁴. When it comes to the IoT, conversely, no 'IoT Act' is on the horizon. This makes it harder to get a clear sense of how this socio-technological phenomenon is being regulated in Europe.

⁶ Florent Thouvenin, Rolf H Weber and Alfred Früh, 'Data Ownership: Taking Stock and Mapping the Issues' in Matthias Dehmer and Frank Emmert-Streib (eds), *Frontiers in Data Science* (CRC Press 2017) 111.

⁷ cf Tommaso Fia, 'An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons' (2021) 21 *Global Jurist* 181.

⁸ European Commission, 'Final Report - Sector Inquiry into Consumer Internet of Things' (n 2) point 24. *Italics mine*.

⁹ Let us only think that, by definition, all Things embed some form of software and the latter is protected by a variety of exclusive rights under copyright (source code, creative interfaces, etc.) and patent law (many of the methods and mechanisms within a Thing will qualify as computer-implemented inventions under the European Patent Convention). On top of these, semiconductor topography rights, trade marks, design rights, trade secrets, and database rights are likely to cover some aspects of a Thing, and to belong to different holders. While the copyright-patent interface has been long studied, the copyright-trademark overlap has been often ignored but it is no less concerning, as argued by Jane C Ginsburg and Irene Calboli, 'Intellectual Property in Transition: The Several Sides of Overlapping Copyright and Trademark Protection' in Niklas Bruun and others (eds), *Transition and Coherence in Intellectual Property Law* (1st edn, Cambridge University Press 2021) 307.

¹⁰ European Commission, Communication 'A European Strategy for Data' (COM/2020/66 final) esp. [3]; and more widely Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data: Rahmenbedingungen Im Europäischen Datenschutz- Und Immaterialgüterrecht Und Übergreifende Reformperspektive* (Mohr Siebeck 2021).

¹¹ Kornrathop Kawintiranon and Yaguang Liu, 'Towards Automatic Comparison of Data Privacy Documents: A Preliminary Experiment on GDPR-like Laws' (arXiv, 20 May 2021) <<http://arxiv.org/abs/2105.10117>> accessed 15 July 2022.

¹² Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence and amending certain union legislative acts (AI Act) (COM/2021/206 final).

¹³ AI Act, art 5.

¹⁴ AI Act, annex III, point 4.

While in the future we expect to see IoT-related interventions in the fields of standard essential patents (SEPs),¹⁵ standards,¹⁶ product liability,¹⁷ and common European data spaces,¹⁸ there are already some instruments that aim to introduce tools to access otherwise locked-up smart data. In this paper, I will focus on the relevant provisions in the Data Governance Act,¹⁹ the Digital Markets Act,²⁰ the Digital Services Act,²¹ and the AI Act, and see how data access and transparency obligations are balanced against IPRs. In previous research I already looked at how this balance is struck under the GDPR²² and the proposed Data Act.²³ Those studies shed light on the emerging conflict between an approach to data governance informed by human rights, sustainability, and social justice – whereby citizens must be given data control, which includes the right to access, reuse, and port the data – and a market-oriented neoliberal one that regards data solely as a commodity to be appropriated and monetised. Other studies have noted how the latest EU law on copyright,²⁴ while introducing text and data mining exceptions, may have inadvertently created new data ownership rights.²⁵ I would like to test now whether those findings can be generalised,²⁶ and in particular whether it can be said that in the European regulation of smart data the reasons of openness are prevailing over those of private property.

¹⁵ While the focus will be on industry-led initiatives, these may be combined with law reforms to improve transparency and predictability in SEP licensing. See European Commission, ‘Making the Most of the EU’s Innovative Potential. An Intellectual Property Action Plan to Support the EU’s Recovery and Resilience’ (2020) COM(2020)760 final.

¹⁶ This strategy includes the objective to ‘(f)oster the development and deployment of international standards for a free, open, accessible and secure global internet and establish an EU internet standards monitoring website’ (European Commission, ‘An EU Strategy on Standardisation Setting Global Standards in Support of a Resilient, Green and Digital EU Single Market’ (2022) COM(2022) 31 final 7.)

¹⁷ Building on European Commission, ‘Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics’ (2020) COM/2020/64 final, the new Product Liability Directive expressly and innovatively regards software as a product (and therefore strict liability will stem from the harm caused by its defects); it also extends the concept of damage to include loss or corruption of data; and moves the foreseeability from the moment the product is put on the market to the moment that the manufacturer loses control over it. See Proposal for a Directive of the European Parliament and of the Council on liability for defective products (Second Product Liability Directive) (COM(2022) 495 final), arts 4(1), 4(6)(c), 4(1)(e).

¹⁸ The rolling-out efforts are currently focused on the creation of European data spaces in the fields of agriculture and mobility, in order to develop a secure and trusted data space to allow these sectors to share and access data, while improving economic and environmental performance. See ‘Common European Data Spaces for Agriculture and Mobility’ (*Digital Strategy Europa*, 13 December 2021) <<https://digital-strategy.ec.europa.eu/en/library/common-european-data-spaces-agriculture-and-mobility>> accessed 18 July 2022.

¹⁹ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act or DGA) [2022] OJ L 152/1.

²⁰ 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 (Digital Markets Act or DMA) [2022] OJ L 265/1.

²¹ 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 (Digital Services Act or DSA) [2022] OJ L 277/1.

²² Guido Noto La Diega and Cristiana Sappa, ‘The Internet of Things at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers’ [2020] REDC 419.

²³ Noto La Diega and Derclaye (n 6).

²⁴ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (C-DSM Directive) [2019] OJ L 130/92, arts 2(2), 3, and 4.

²⁵ Thomas Margoni and Martin Kretschmer, ‘A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology’ (2022) 71 GRUR International 685.

²⁶ There is an unavoidable margin of discretion in the definition of the scope of analysis. Future research should also consider other legal instruments, namely Directive (EU) 2016/680 (Law Enforcement Directive), art 14

2. Opening up smart data held by public sector bodies

The IoT is transforming the public sector,²⁷ as epitomised by the abundance of investments in smart cities,²⁸ and the work being done to build a public, open, and secure data infrastructure to regain digital sovereignty in the EU²⁹. As the amount of publicly-held smart data, it become crucial to explore the accessibility and re-usability of this data by citizens. Thirty-five years after the FOIA,³⁰ the EU adopted the Directive on the Re-Use of Public Information³¹ with the purpose of regulating access to and re-use of documents held by public sector bodies of the Member States. Replaced in July 2021, the Open Data Directive³² has a broader scope as it encompasses also documents held by publicly controlled enterprises³³ and data generated by publicly funded research.³⁴ Despite such positive embracing of openness, the new law does not apply to documents for which third parties hold IPRs³⁵ as well as ‘documents, such as sensitive data, which are *excluded from access* by virtue of the access regimes in the Member State, including on grounds of [...] commercial confidentiality.’³⁶ This signals a clear tension between the tendency of framing data privacy as a fundamental human right, and its commodification. While this is usually the consequence of how private business encloses and extracts value from the data generated by the IoT, public entities are often at fault too as IP-protected documents and data are too ‘often not made available, not even for research or innovative activities.’³⁷ Therefore, it is positive news that in May 2022³⁸ – as part of the European strategy for data³⁹ – the Data Governance Act was passed and set to create robust mechanisms to facilitate the reuse of certain categories of protected public-sector data.

(Right of Access by the Data Subject); Regulation (EU) 2018/1725 (European Institutions Data Protection Regulation), art 17 (Right of Access by the Data Subject), art 22 (Right to Data Portability); Directive (EU) 2019/1024 (Open Data Directive) art 4 (Processing of requests for re-use); Directive 2003/4/EC (Environmental Information Directive), art 3 (Access to environmental information upon request); draft Platform Work Directive, arts 6, 12 (access to information about algorithmic systems by workers, and about digital labour platforms more generally); draft European Health Data Space Regulation, arts 3, 4, 45-49 (Access to and transmission of personal electronic health data for primary use; access by health professionals to personal electronic health data; data access for secondary use).

²⁷ See e.g. Ulrika H Westergren, Katrin Jonsson and Ott Velsberg, ‘Internet of Things in the Public Sector. Perspectives from Northern Europe’ (2019) Department of Informatics RR19.02.. The authors warn that ‘since the application of IoT within the public sector can lead to a potential invasion of privacy for individual citizens, it is important to have established clear ethical guidelines and to keep an eye of both opportunities and downsides to IoT implementation’ (ibid 14).

²⁸ Over the years, the European Commission has been funding large-scale pilots to create resilient and carbon-neutral smart cities and smart rural communities. See e.g. pilots SynchroniCity, MONICA, VICINITY, AURORAL, and dRural. National and local investments in smart cities also abound, see e.g. Barcelona’s Digital City plan revolving around the idea of public data commons.

²⁹ The reference is to Gaia-x; see Francesco Bonfiglio, ‘Vision & Strategy’ (2022) Gaia-X.

³⁰ The Freedom of Information Act, 5 U.S.C. § 552.

³¹ Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information [2003] OJ L 345/90.

³² Directive (EU) 2019/1024, art 19.

³³ This law applies to any enterprises active in certain sectors (e.g. water, energy, transport and postal services) over which the public sector bodies exercise a dominant influence (Open Data Directive, arts 1(1)(b) and 2(3)).

³⁴ Publicly funded research data has to be openly available and re-usable for commercial or non-commercial purposes, with the limitations set forth by Article 10 of the Open Data Directive (one of them being the necessity to take into account concerns relating to IPRs).

³⁵ Open Data Directive, art 1(2)(c).

³⁶ Open Data Directive, art 1(2)(d)(iii).

³⁷ Data Governance Act, recital 5. For the US readers, it is worth mentioning that recitals are the non-binding part of European legal instruments that perform an important function as interpretive aid. See e.g. Llio Humphreys and others, ‘Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation.’ (2015).

³⁸ The new law will become applicable in September 2023.

³⁹ European Commission, ‘A European Strategy for Data’ (2020) COM/2020/66 final.

Crucially, the new law applies also to data that is protected on grounds of commercial confidentiality and IP.⁴⁰

Unlike the Open Data Directive, the Data Governance Act is not limited to research data, it applies to any data, broadly defined as ‘any digital representation of acts, facts or information and any compilation of such acts, facts or information.’⁴¹ A first conflict to resolve is between the statement that the new law applies to IP-protected and confidential data, and the provision whereby the Act does ‘not create any obligation on public sector bodies to allow re-use of data nor do they release public sector bodies from their confidentiality obligations.’⁴² Let us give a closer look at the law to appreciate whether this contradiction can be overcome.⁴³

The ethos of openness⁴⁴ in the Data Governance Act revolves around the requirement that public sector bodies set forth publicly available, non-discriminatory, proportionate, pro-competitive, and objectively justified conditions for the re-use of data⁴⁵. This means that these organisations can decide not to allow the re-use but if they do allow it they have to do so pursuant to conditions having the aforementioned features. The balance between IP and access appears to be struck in favour of the former. Indeed, on the one hand, the Act provides that public sector bodies cannot exercise the database right to prevent re-use of data⁴⁶. On the other hand, however, re-use is only allowed in compliance with IPRs and confidentiality.⁴⁷ The preservation of the protected nature of data is delegated to technology; namely, public sector bodies may be required to deploy disclosure control techniques and to allow access within secure processing environments.⁴⁸ Additionally, the new law imports the model that the GDPR introduced with regard to international data transfers. Similar to the adequacy decisions the European Commission takes to recognise that the level of data protection is essentially

⁴⁰ Data Governance Act, art 3(1)(a) and (c).

⁴¹ Data Governance Act, art 2(1).

⁴² Data Governance Act, art 3(3).

⁴³ Other commentators have underlined that this new law creates legal uncertainty because it is unclear how it will interact with other areas of law. For example, with a focus on the interactions with the GDPR, competition law, and the Digital Markets Act, see Inge Graef and Raphael Gellert, ‘The European Commission’s Proposed Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing’ (2021) TILEC Discussion Paper No. DP2021-006 <<https://papers.ssrn.com/abstract=3814721>> accessed 20 July 2022. Another ground of criticism is the lack of clarity as to what ‘data governance’ means, which is a key argument in Maximilian Grafenstein, ‘Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as Well as the GDPR)’ (2022) HIIG Discussion Paper Series No. 2022-02 <<https://papers.ssrn.com/abstract=4104502>> accessed 20 July 2022.

⁴⁴ Other provisions may be relevant but, due to word limit constraints, will have to be the subject of future research e.g. Article 4, that prohibits exclusive arrangements granting exclusive rights over data or restricting the availability of data for re-use by entities other than the parties to these agreements. An analysis can be found in Giulia Schneider, ‘Data Sharing for Collaborative Research under Art. 101 TFEU: Lessons from the Proposed Regulations for Data Markets’ (2021) 17 European Competition Journal 567.

⁴⁵ Data Governance Act, art 5(1)-(2).

⁴⁶ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20, art 7. In the EU, databases are protected both by copyright (but the originality requirement is seldom made out) and by the database right or sui generis right, which is the right to prevent extraction and re-utilisation of substantial parts of a database, provided that there is evidence of a substantial investment in obtaining, presenting, or verifying its contents. The most comprehensive account on IP and databases in Europe remains Estelle Derclaye, *The Legal Protection of Databases: A Comparative Analysis* (Edward Elgar 2008).

⁴⁷ Data Governance Act, art 5(7)-8).

⁴⁸ This may be regarded as another instance of technological solutionism, a trend that the COVID-19 pandemic has exacerbated as correctly noted by David Lyon, *Pandemic Surveillance* (Polity Press 2022) 14–16.

equivalent to the European one⁴⁹ – in which case personal data can be exported (the US being no longer one of the valid destinations after *Schrems II*)⁵⁰ – the Data Governance Act entrusts the Commission with the power to adopt ‘adequacy declarations’.⁵¹ The adequacy declarations will confirm that: (i) the foreign country ensures an essentially equivalent protection of IPRs and trade secrets; (ii) the relevant laws and supervisory arrangements are effectively applied; (iii) judicial redress is effective.⁵²

The pro-proprietary approach is tempered by four factors. First, the idea of IP-protected data would surprise any European IP scholar. Indeed, it has become close to undisputable that there is no property and no IP over data as such.⁵³ What come near the idea of data property are the database right – but the Data Governance Act provides that public sector organisations cannot rely on it to prevent the reuse of data – and data exclusivity. The latter refers to TRIPs Plus provisions in bilateral trade agreements that impose additional obligations to keep certain data (typically trial data) secret.⁵⁴ However, this is not likely to be relevant in the context of public smart data as it normally regards the commercial pharmaceutical sector.⁵⁵

Second, there is no consensus as to whether trade secrets can cover smart data.⁵⁶ The main obstacle is that the users of a Thing can easily access the data in the Thing and this would run counter a key requirement under trade secrecy in the EU i.e. the fact that the holder of the information must have taken reasonable steps to keep the information secret via technical, organizational, and contractual barriers.⁵⁷ Apart from the fact that, increasingly, smart data is processed in the cloud, the supposed ease of access of smart data stored in the Thing does not necessarily extinguish trade secrecy. Lessons can be learned from the case law regarding encrypted confidential information posted online. On the one hand, it constitutes traditional teaching that if the data in the public domain needs reverse engineering, it has to be treated as relatively secret.⁵⁸ On the other hand, courts have now for some time recognised that encryption is not as such a sufficient step to keep data secret. Indeed, as stated in *Mars v Teknowledge*,⁵⁹

⁴⁹ GDPR, art 45. There are a number of ways a data export can be justified, including standard contractual clauses and binding corporate rules. For an analysis that also considers the complexities stemming from the UK’s withdrawal from the EU see Karen Mc Cullagh, ‘Post-Brexit Data Protection in the UK’ in Rosamunde van Brakel, Paul de Hert and Gloria González Fuster (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar 2021).

⁵⁰ Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* ECLI:EU:C:2020:559, that invalidated the adequacy decision pertaining US-EU data flows, known as ‘Privacy Shield’ (which in turn replaced its predecessor, the ‘Safe Harbor’ decision that the Court of Justice declared invalid in Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650). cf Rachel F Fefer and Kristin Archick, ‘EU Data Protection Rules and U.S. Implications’ (2021) 32 *Current Politics and Economics of Europe* 255.

⁵¹ Data Governance Act, art 5(9), which refers to them as ‘implementing acts’.

⁵² Data Governance Act, art 5(9)(a)-(c).

⁵³ In 2017, the European Commission proposed the introduction of a new data ownership right, which led to a nearly unanimous outcry. On the debate see Jacopo Ciani, ‘A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider “Holistic Approach”’ in Mor Bakhoun and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (Springer 2018).

⁵⁴ Lisa Diependaele, Julian Cockbain and Sigrid Sterckx, ‘Raising the Barriers to Access to Medicines in the Developing World - The Relentless Push for Data Exclusivity’ (2017) 17 *Developing World Bioethics* 11.

⁵⁵ Fabian Gaessler and Stefan Wagner, ‘Patents, Data Exclusivity, and the Development of New Drugs’ [2020] *The Review of Economics and Statistics* 1.

⁵⁶ For an analysis of the point see Noto La Diega and Sappa (n 23).

⁵⁷ Trade Secrets Directive, recitals 7, 12 and art 2(1)(c). This is different to TRIPS, art 39, as noted by Gintarė Surblytė, ‘Enhancing TRIPS: Trade Secrets and Reverse Engineering’ in Hanns Ullrich and others (eds), *TRIPS plus 20: From Trade Rules to Market Principles* (Springer 2016) 725.

⁵⁸ *Ackroyds v Islington Plastics* [1962] RPC 97, 104.

⁵⁹ [2000] FSR 138, which deals with the common law of breach of confidence.

anyone can acquire the skills to decrypt and access encrypted information or hire someone with the necessary skills.⁶⁰ Therefore, one could not regard as secret the information that is embodied in an object that, being in the public domain, can be easily accessed through reverse engineering⁶¹. Accordingly, one may argue that the data that is embodied in Things is not secret, as long as it can be easily accessed by means of reverse engineering or decrypted.⁶²

Third, data access is facilitated through a remote-access-by-default approach. Public sector organisations can demand that data is accessed and re-used within its own physical premises only if ‘remote access cannot be allowed without jeopardising the rights and interests of third parties’.⁶³ In most instances, online access can be designed in ways that do not compromise the protected nature of data. For example, if the terms and conditions include a confidentiality clause, the disclosure of data in breach of those terms will not lead to a loss of protection under both patent law⁶⁴ and confidentiality law⁶⁵. Additionally, there are a variety of techniques that allow for the sharing of data without affecting its nature e.g. random perturbation and data swapping⁶⁶.

Fourth, potential re-users of publicly-held smart data do not necessarily have to wait for an adequacy declaration to certify that a non-EU country provides an essentially equivalent level of IP protection. As we have seen with the adequacy decisions provided by the GDPR, it can take the European Commission an extremely long time to adopt them, and as the *Schrems* saga shows there is no legal certainty even after their adoption. Therefore, it is praiseworthy that the Data Governance Act provides that the re-use of data can take place also in foreign countries that are not covered by adequacy declarations as long as the re-user undertakes to (i) accept the jurisdiction of one of the EU’s Member States, and (ii) to comply with IP law – which, as seen in prior passages, has limited application to data – and with the law of confidence – which has disputed application to the IoT.⁶⁷

Overall, it can be said that the new openness requirements set forth by the Data Governance Act with regard to IP-protected and confidential data held by public entities are a step forward and continue advancing the ‘idea that data that has been generated at the expense of public

⁶⁰ibid 149.

⁶¹ *Saltman Engineering Co v Campbell Engineering Co* (1948) 65 R.P.C. 203

⁶² However, courts have become in more recent times amenable to the idea of considering Thing-embedded algorithms as secret e.g. *Volkswagen v Garcia* [2013] EWHC 1832 (Ch). It is too early to say which stream of jurisprudence will prevail.

⁶³ Data Governance Act, art 5(3)(c).

⁶⁴ For an invention to be patented it must be novel i.e. not the subject of a prior enabling disclosure (enabling meaning that the person skilled in the art can work the disclosed invention) (Patents Act 1977, s 2). However, the disclosure will be disregarded if made in breach of confidence (Patents Act 1977, s 2(4)(a), (b); *Threeway Pressings Ltd’s Application* [2012] RPC 129 BL O/124/12).

⁶⁵ In the UK, this is due to the principle of relative secrecy. Unlike patent law – where virtually any disclosure can prevent the novelty requirement from being made out (e.g. *H.Lundbeck A/S v Norpharma SpA* [2011] EWHC 907 (Pat), [2011] RPC 23 about implicit disclosures) – in the law of breach of confidence, information that is available to the public can still be protected if not sufficiently widely known (*R (on the application of Ingenious Media Holdings) v Revenue and Customs Commissioner* [2016] UKSC 54 [25]). Amongst other things, this principle is at the basis of the springboard doctrine, whereby a person who has obtained information in breach of confidence should not be allowed to use it as a springboard for activities detrimental to the competitor (*Vestergaard Frandsen A/S (now called MVF 3 Aps) v Bestnet Europe Ltd* [2016] EWCA Civ 541). The UK is composed of three legal systems i.e. England and Wales, Scotland, Northern Ireland. I refer to the UK as the law of confidence is considered to be the same in all jurisdictions (*Lord Advocate v Scotsman Publications Ltd* 1989 SC (HL) 122, 162-163; *AB v Sunday Newspapers (t/a The Sunday World)* [2014] NICA 58 [19]-[24]).

⁶⁶ See Barbara Helmecht and Daniela Schackis, *Manual on Disclosure Control Methods* (Office for Official Publications of the European Communities 1996).

⁶⁷ Data Governance Act, art 10.

budgets should benefit society.’⁶⁸ It is understandable that, to strike a balance between data access and IP certain technical and legal procedural requirements must be met before public smart data is made available, but it important that the anti-proprietary elements in the new law and the limitations inherent to data property be adequately exploited if we want the data generated by smart cities, smart urban communities, etc. to be re-used for the common good. Unfortunately, the ‘para-IP’ created by technological protection measures and the absence of a proper data access right (let alone an access duty) substantiate the concern that the policy objective to open up publicly held data may end up being frustrated by proprietary considerations.

3. Data access for fairer, open, and contestable digital markets

Regrettably, the Data Governance Act does not introduce access rights or positive obligations to allow data access. The same cannot be said for the Digital Markets Act aimed at constraining the behaviour of the largest digital companies to gatekeep the internet. Adopted in September 2022, the new law applies to these ‘gatekeepers’ if they (i) have a significant impact on the EU’s internal market; (ii) provide a core platform service; and (iii) enjoy or are likely to enjoy an entrenched and durable position⁶⁹. US readers will be interested to learn that this Act will apply also to foreign providers of core platform services if the business users⁷⁰ are established in the EU or the end-users are established or located in the Union.⁷¹ This Act was meant to build on the evidence coming from the IoT inquiry,⁷² but it is unclear whether those findings have in any way influenced the relevant law-making process. It would seem that they partly did, at least as one of the differences between the proposal and the final text is the addition of provisions related to virtual assistants as a core platform service, which means that the relevant providers will fall within the subjective scope of the Digital Markets Act. Arguably, IoT companies were already within the scope as they can offer online intermediation services, cloud computing services, and ‘number-independent interpersonal communications services.’⁷³ The latter category – created to make sure that communication services such as Skype and Telegram could not sidestep telecom regulations – is problematic from an IoT standpoint as it excludes the exchange of information between machines.⁷⁴ However, as long as the service allows the recipient of the information to respond, the ‘interactivity’ requirement is made out⁷⁵ and Things like Amazon Echo or Google Home will be regarded as number-independent interpersonal communications services falling within the scope of the new law.

⁶⁸ Data Governance Act, recital 5.

⁶⁹ Digital Markets Act, art 3(1).

⁷⁰ ‘Business user’ means ‘any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users’ (art 2(17)).

⁷¹ Digital Markets Act, art 1(2).

⁷² European Commission, ‘Staff Working Document SWD(2022) 10 Final’ (n 2) 8.

⁷³ Digital Markets Act, art 2(2)(e). This provision refers to the European Electronic Communications Code for the definition of ‘interpersonal communications services’ as ‘services that enable interpersonal and interactive exchange of information, covering services like traditional voice calls between two individuals but also all types of emails, messaging services, or group chats’ (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, recital 17). The Act itself defines ‘number-independent’ as not connecting with publicly assigned numbering resources (Digital Markets Act, art 2(7)). The nature of these over-the-top (OTT) services was previously disputed, as exemplified by the divergence between Case C-193/18 *Google LLC v Bundesrepublik Deutschland* EU:C:2019:498 (rejecting the qualification of Gmail as an electronic communications service) and Case C-142/18 *Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (‘IBPT’)* EU:C:2019:460 (qualifying SkypeOut as an electronic communications service).

⁷⁴ Digital Markets Act, recital 17.

⁷⁵ *ibid.*

Having clarified that the Digital Markets Act applies to IoT companies acting as digital gatekeepers, it is important to look at how a new access right can be pivotal to the Act pursuing its objectives of fair, open, and contestable digital markets.⁷⁶ The core provision in this sense is data portability. Complementing the right to portability of personal data provided by the GDPR,⁷⁷ the Act appears to move away from a rights-based approach – where enforcement relies on under-resourced and under-informed end-users to exercise their rights⁷⁸ – as it introduces a portability obligation. In particular, the IoT gatekeeper will have to put in place systems that allow end users to port, free of charge, the data they provided or generated through their activity in the context of the relevant core platform service (e.g. virtual assistance).⁷⁹ Peculiarly perhaps, data access – that shall be continuous, in real time, effective, and immediate⁸⁰ – is framed as ancillary to portability, i.e. as one of the ‘tools to facilitate the effective exercise of such data portability.’⁸¹

While a fully autonomous obligation would have been a more welcome innovation, it ought to be regarded as positive – from the perspective of overcoming smart data enclosures – that the Act does not appear to counterbalance these obligations with IP and confidentiality in a way that would sterilise its ethos of openness. Four elements point in this direction. First, the technical measures that are too often used to create or strengthen monopolies over data⁸² are here mandated as enablers of continuous portability (e.g. through high-quality interfaces).⁸³ Second, the lawmaker expressly considered the interplay between the Act and other laws when it provided that in setting up systems to comply with the new obligations, the gatekeepers retain compliance with ‘applicable law,’⁸⁴ expressly identified in accessibility requirements, data protection and cybersecurity, consumer protection, and product safety. The fact that accessibility features prominently and IP is missing is a clear indication of a policy stance against data enclosures. This is further corroborated by a third consideration. The EU Institutions, in drafting and discussing the Act, have indeed taken into account IP and confidentiality, but only with regard to other aspects of the new regulation. Most prominently,⁸⁵

⁷⁶ Other mechanisms provided in this Act include the prohibition of a number of unfair practices e.g. blocking users from uninstalling pre-installed software and sanctions going beyond the mere fines, including structural measures e.g. divestiture orders. This is to be welcome as positive considering that big tech has proved to be immune to even large fines imposed under the GDPR. See e.g. W Gregory Voss and Hugues Bouthinon-Dumas, ‘EU General Data Protection Regulation Sanctions in Theory and in Practice’ (2020) 37 Santa Clara High Technology Law Journal.

⁷⁷ GDPR, art 20; Digital Markets Act, recital 59.

⁷⁸ For a critique of the GDPR’s rights-based approach, see Rachel Allsopp, ‘Levelling the Odds? Big Data Analytics in the Online Gambling Industry and the Application of the GDPR’ in MM Carvalho (ed), *Law & Technology. E.Tec Yearbook* (University of Minho 2018).

⁷⁹ Digital Markets Act, art 6(9).

⁸⁰ Digital Markets Act, art 6(9); recital 59.

⁸¹ Digital Markets Act, art 6(9).

⁸² European Innovation Council and others, *Study on the Legal Protection of Trade Secrets in the Context of the Data Economy: Final Report* (Publications Office of the European Union 2022) <<https://data.europa.eu/doi/10.2826/021443>> accessed 7 October 2022.

⁸³ Digital Markets Act, recital 59.

⁸⁴ Digital Markets Act, art 8(1).

⁸⁵ Other relevant provisions are recitals 88-89 (on the respect of confidentiality in the publication of any decisions against gatekeepers), art 8 (on (i) the non-confidential submission that the gatekeeper can provide to the Commission to explain the measures that it intends to implement to comply with the new obligations, and (ii) the publication of a non-confidential summary of the case), art 11 (annual non-confidential summary of the report about how the gatekeeper has complied with the new obligations), art 18 ((i) non-confidential summary of the preliminary findings and remedies in the event of market investigations by the Commission for suspected systematic non-compliance; (ii) publication of non-confidential summary of the case and the commitments offered by the gatekeeper and made binding by the Commission), art 34 (confidentiality in the context of the right to be heard and access to the file), art 38 (exchange of confidential information between the Commission and the

the Act introduces measures to protect whistle-blowers (or anyone wishing to complain about an unfair practice), seen as pivotal to the fairness and contestability of the digital markets. The lawmaker shows awareness of the practices that use non-disclosure agreements as gagging instruments and expressly prohibits any ‘confidentiality clauses in agreements or other written terms’⁸⁶ that could inhibit or hinder these complaints. Fourth, crucially, the obligation to put in place systems for continuous and real-time access means that the lawmaker has chosen access over IP, openness over closure. Indeed, it has been argued that the GDPR excludes real-time access to personal data if trade secrets are at play as it would be impossible to retain confidentiality under those conditions.⁸⁷ It follows that the new obligation signals a clear policy choice in favour of access and against proprietary considerations.

It has been predicted that this regulation may have ‘major, maybe revolutionary, implications on some of the business models of the largest firms worldwide.’⁸⁸ We will be able to tell in a not too distant future; in the meantime, it seems clear that the Act is a positive step forward in the direction of dismantling smart data enclosures by (i) shifting from rights-based approaches to duty-based ones; and (ii) taking a clear policy stance in favour of openness (via portability and access) and against proprietary considerations. At the same time, the construction of data access as merely ancillary to portability can be exploited by IoT gatekeepers to reject access requests that are not linked to portability. Indeed, while the goal to balance openness and IP is a justifiable one, in practice it allows powerful IoT players to leverage their IPRs and technological dominance to (ab)use IP as a way to prevent enclosed data from being re-used for the common good.

4. Curbing the power of digital services platforms through independent audits and data access by regulators

The Digital Markets Act is complemented by the Digital Services Act.⁸⁹ Both apply extraterritorially, i.e. also to US companies with customers in the EU.⁹⁰ Adopted in October 2022, this Act has been celebrated⁹¹ as the most important legal intervention in the field of e-commerce law since 2000,⁹² when the EU (then European Community) introduced rules on intermediary liability similar to the Digital Millennium Copyright Act⁹³ and the Communications Decency Act.⁹⁴ In introducing positive and negative due diligence obligations

national competent authorities), art 44 (publication of final decisions, which shall have regard to the legitimate interest of gatekeepers and third parties in the protection of confidentiality).

⁸⁶ Digital Markets Act, recital 42.

⁸⁷ Noto La Diega and Sappa (n 23).

⁸⁸ Pierre Larouche and Alexandre de Streel, ‘The European Digital Markets Act: A Revolution Grounded on Traditions’ (2021) 12 *Journal of European Competition Law & Practice* 542. The authors do nonetheless note that the policy options are quite traditional.

⁸⁹ They are collectively known as the Digital Services Package.

⁹⁰ Or, in the words of the Digital Services Act, provided that the ‘recipients of the service (...) have their place of establishment or are located in the Union’ (art 2(1)).

⁹¹ Not without a critical appraisal, Caroline Cauffman and Catalina Goanta, ‘A New Order: The Digital Services Act and Consumer Protection’ (2021) 12 *European Journal of Risk Regulation* 758.

⁹² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’ or ‘e-Commerce Directive’) [2000] OJ L 178/1.

⁹³ Section 512) of the United States Copyright Act. For a comparison see Lia Shikhiashvili, ‘The Same Problem, Different Outcome: Online Copyright Infringement and Intermediary Liability under US and EU Laws’ (2019) 24 *Intellectual Property and Technology Law Journal* 125.

⁹⁴ Section 230(c). Cf. Trent Scheurman, ‘Comparing Social Media Content Regulation in the US and the EU: How the US Can Move Forward with Section 230 to Bolster Social Media Users’ Freedom of Expression Comments’ (2021) 23 *San Diego International Law Journal* 413. More widely, Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar Publishing 2020).

for a range of platforms,⁹⁵ the Digital Services Act aims at ensuring that the relevant services are not used for illegal activities and that private operators act responsibly. In doing so, this Act in principle maintains the ‘safe harbour’ approach of previous legislation, but it forces online intermediaries to become more ‘(r)esponsible and diligent’⁹⁶ with the ultimate goal to achieve a fundamental-rights-compliant, innovative, ‘safe, predictable and trusted online environment.’⁹⁷ Even though an open environment is not expressly referred to, it is worth mentioning that the Act expressly refers to the importance for European citizens to be able to exercise their freedom of expression, and that the latter includes the freedom to receive information.⁹⁸ Additionally, the reference to the Charter of Fundamental Rights of the EU by necessity includes the right to the protection of personal data, which in turn encompasses the right of access to data.⁹⁹ A problematic profile may pertain non-personal data. Indeed, while freedom to receive information can be construed as to cover access to non-personal data, it remains unclear whether it can be extended to encompass the freedom to port or more generally re-use non personal data.

Codifying the increasing judicial pressure and enforcement focus on bigger platforms – pursuant to the Marvel principle whereby with great power comes great responsibility¹⁰⁰ – the Digital Services Act introduces new obligations that are modulated based on the type (and the size) of intermediary.¹⁰¹ So for example, the providers of intermediary services (e.g. hosting) have obligations to make publicly available transparency reports on a number of issues e.g. moderation practices, including the use of automated tools.¹⁰² Online platforms,¹⁰³ in turn, must provide that the moderation decisions can be reviewed ‘under the supervision of appropriately qualified staff.’¹⁰⁴ Finally, big tech companies are the subject of more stringent requirements. These ‘Very Large Online Platforms’ (VLOP) – so designated if they have at least 45 million monthly active users in the EU¹⁰⁵ – must inter alia open themselves to independent audits¹⁰⁶ and allow access to data for public enforcement purposes.¹⁰⁷

⁹⁵ See e.g. the duty to set up internal complaint-handling systems (Digital Services Act, art 20) and the ban on dark patterns (recital 67), respectively.

⁹⁶ Digital Services Act, recital 3.

⁹⁷ Digital Services Act, art 1(1). It has been noted that if we want to minimise the impact of emerging technologies on fundamental rights we need to move away from traditional data protection approaches and focus on risk-based approaches through more holistic and participatory impact assessments (Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Asser Press 2022).

⁹⁸ Charter of Fundamental Rights of the EU (CFREU), art 11(1).

⁹⁹ CFREU, art 8(2). I will not consider the interplay between this new regime and copyright, which is the subject of João Pedro Quintais and Sebastian Felix Schwemer, ‘The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?’ (2022) 13 *European Journal of Risk Regulation* 191.

¹⁰⁰ Lilian Edwards, “‘With Great Power Comes Great Responsibility?’ The Rise of Platform Liability’ in Lilian Edwards (ed), *Law, policy and the Internet* (Hart 2019).

¹⁰¹ While this asymmetric structure of obligations reflects the central role of big tech in online intermediation, it underestimates the threats posed by smaller platforms, as noted by Buiten (n 102) para 70.

¹⁰² Digital Services Act, arts 15 (esp. 15(1)(c)).

¹⁰³ Only some hosting providers qualify as online platforms, i.e. those ‘that, at the request of a recipient of the service, store[...] and disseminate[...] information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation’ (Digital Services Act, art 3(i))

¹⁰⁴ Digital Services Act, art 20(6).

¹⁰⁵ Digital Services Act, art 33(1).

¹⁰⁶ Digital Services Act, art 37.

¹⁰⁷ Digital Services Act, art 40.

As the IoT heavily relies on intermediaries (e.g. PTC ThingWorx, AWS IoT Core, Microsoft Azure IoT, etc.),¹⁰⁸ there is no doubt that the Digital Services Act should be analysed to critically assess whether the objective to creating a more responsible internet through platform regulation¹⁰⁹ includes the overcoming of smart data enclosures, and if the latter is neutralised through IP balancing and other proprietary and quasi-proprietary tools.

I will zoom in on these two VLOP-specific mechanisms as, on the one hand, they provide incentives for private business to adopt more openness in their data practices; on the other hand, they would appear to provide enclosure tools by way of IPRs. Previous research has shown that large transnational corporations tend to behave like ‘black boxes’ (regardless of whether they adopt opaque AI systems), as they operate under minimum transparency requirements and fully embrace factual secrecy.¹¹⁰ Coupled with technical and IP-related opacities, this has been referred to as the ‘triple black box’ of the algorithms that are weaved into our world.¹¹¹ Against this backdrop, the duty for VLOPs to open up to independent audits to assess compliance with the new obligations (and commitments under codes of conduct and crisis protocols) appears to be a praiseworthy one, especially as it expressly includes a requirement to give auditors ‘access to all relevant data.’¹¹² However, there are at least three limitations to the potential of this provision to overcome or at least challenge smart data enclosures. First, there is no way to rule out data curation, namely the discretionary decision, by the VLOP, of what data counts as ‘relevant.’ Second, the auditor has to ensure an ‘adequate level of confidentiality and professional secrecy’¹¹³ in respect of the information obtained in the context of the audits. This is only partly an issue as the Act as the latter is clear that complying with the requirements of confidentiality and secrecy is no carte blanche as it cannot adversely affect the performance of the audits (as well as the provisions of the new law about transparency, supervision and enforcement). Third, the wider and perhaps more fundamental problem is that the architecture of the Digital Services Act epitomises a new trend in the EU approach to regulating technologies; notably, the outsourcing of regulatory powers to private parties.¹¹⁴ Indeed, the identification and solution of risks is in the first instance left to the VLOP – that will have to carry out a yearly self-assessment of any significant systemic risks caused by their services¹¹⁵ – and compliance is outsourced to private audit firms, whose final recommendations are by their very nature not binding.¹¹⁶

The tension between access and property can be further observed through the lens of the new duty for VLOPs to give the European Commission or the relevant Digital Services

¹⁰⁸ ‘Industrial IoT Platforms Reviews 2022’ (Gartner, 2022) <<https://www.gartner.com/market/industrial-iot-platforms>> accessed 11 October 2022.

¹⁰⁹ Miriam C Buiten, ‘The Digital Services Act from Intermediary Liability to Platform Regulation’ (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 361; Andrej Savin, ‘The EU Digital Services Act: Towards a More Responsible Internet’ (16 February 2021) <<https://papers.ssrn.com/abstract=3786792>> accessed 11 October 2022.

¹¹⁰ Maayan Perel and Niva Elkin-Koren, ‘Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement’ (2017) 69 Fla. L. Rev. 181; Sharon K Sandeen and Tanya Aplin, ‘Trade Secrecy, Factual Secrecy and the Hype Surrounding AI’ in Ryan Abbott (ed), *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar 2022).

¹¹¹ Guido Noto La Diega, ‘Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information’ (2018) 9 JIPITEC 3.

¹¹² Digital Services Act, art 37(2).

¹¹³ Digital Services Act, art 37(2).

¹¹⁴ This is a point convincingly made by Cauffman and Goanta (n 92) 770.

¹¹⁵ Digital Services Act, art 34(1).

¹¹⁶ If the VLOP decides to ignore the report of the auditor, they will simply have to justify ‘in the audit implementation report the reasons for not doing so and set out any alternative measures they have taken to address any instances of non-compliance identified’ (art 37(6))

Coordinator¹¹⁷ ‘access to data that are necessary to monitor and assess compliance’¹¹⁸ with the Digital Services Act. Access shall be facilitated through appropriate interfaces, including online databases and application programming interfaces.¹¹⁹ This is a potentially important provision, especially as this access duty includes inter alia ‘the data necessary to assess the risks and possible harms brought about by the platform’s or search engine’s systems, data on the accuracy, functioning and testing of algorithmic systems for content moderation, recommender systems or advertising systems, including, where appropriate training data and algorithms, or data on processes and outputs of content moderation or of internal complaint-handling systems.’¹²⁰ While it is regrettable that end-users cannot directly benefit from this duty, the Commission and the Digital Service Coordinators, if resourced appropriately, may be able to use public enforcement to force IoT intermediaries to lower the fences enclosing their data. The regulators are asked to ‘take due account of the rights and interests of the [VLOPs] including [...] the protection of confidential information, in particular trade secrets.’¹²¹ However, this would not justify blanket refusals to data access requests based on actual or alleged IPRs on smart data (or the relevant algorithms). Two arguments militate in favour of this conclusion. First, this caveat is included in a paragraph related to the use of the data, once accessed, not the access itself. This means that while access cannot be denied, the data will have to be handled in a way that does not adversely affect its confidential nature, and that more generally nullifies the proprietary interests of the platform. The regulators will have to put in place organisational, technical, and contractual measures to this effect. Second, in the original text of the proposed Digital Services Act, VLOPs were entitled to ask the regulators to amend their data access requests if ‘giving access to the data [would have led] to significant vulnerabilities for the [...] protection of confidential information, in particular trade secrets.’¹²² This could have indeed been construed as a *carte blanche* for VLOPs to tighten their grips over smart data. However, in the version adopted by the European Parliament, this condition only applies to requests coming from researchers, which by contrast means that VLOPs cannot oppose regulators’ requests. And even when we are dealing with access requests coming from researchers, VLOPs cannot simply deny them; indeed, they have to propose ‘one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.’¹²³

All in all, the Digital Services Act provides strong incentives to open up enclosed data. On the one hand, it has some drawbacks, notably the fact that openness is expressly included in the objectives of the Act (with practical consequences in terms of re-using non-personal data), the outsourcing of regulatory powers to private parties, the leaving end-users out of the picture and not doing much about private remedies.¹²⁴ On the other hand, it is commendable for its duty-

¹¹⁷ EU Member States are tasked with designating one or more competent authorities to supervise online intermediaries and enforce the new law; one of them will be the Digital Services Coordinator, who will be responsible for supervising and enforcing the Act and coordinating the national authorities (Digital Services Act, art 49). The provision on data access refers to Digital Services Coordinator of establishment, i.e. of the EU Member State where the main establishment of a provider of an intermediary service is located or its legal representative resides or is established (art 3(n)).

¹¹⁸ Digital Services Act, art 40(1).

¹¹⁹ Digital Services Act, art 40(7).

¹²⁰ Digital Services Act, recital 96.

¹²¹ Digital Services Act, art 40(2).

¹²² Proposed Digital Services Act, art 31(6)(b). The text of the proposal, dated 15th December 2020, is available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0825&qid=1665480452415>> accessed 11 December 2022.

¹²³ Digital Services Act, art 40(6).

¹²⁴ Private enforcement is not irrelevant even though in the context of locked-in and vulnerable IoT consumers one can expect public enforcement to play a more important role. I would nonetheless agree that ‘a European legal

based approach, the strengthened public enforcement,¹²⁵ and the fair balance between access and property resulting from the obligation to consider IP when it comes to the use of data, as opposed to its access. It has been argued that even though the US do not have similar legislation in place, the ‘Brussels effect will push [foreign] private enterprises to comply and give rise to similar legislative initiatives.’¹²⁶ While no such initiatives appear to be on the horizon, one would hope that extra-EU lawmakers will be inspired by the positive aspects of the new law while avoiding the aforementioned drawbacks.

5. The Artificial Intelligence Act: countering technological risk through access to training data and source code

As the smart data enclosures – and the ensuing opacity and fragmentation of the IoT – are connected also to the growing embedding of AI technologies into cyber-physical systems,¹²⁷ it is worth shifting our focus to the latest attempt by the EU to become a global leader in digital regulation,¹²⁸ notably the AI Act.¹²⁹ Similar to the legislation analysed in the previous sections, US-based providers of AI systems will be subject to the proposed regulation if (i) they place the system on the EU market (or otherwise put it into service), (ii) their users are EU-based, or (iii) the output produced by the system is used in the EU.¹³⁰ The application to the IoT is straightforward, as AI systems are defined broadly and encompass systems that are ‘*physically integrated into a product (embedded)*’¹³¹ and whose ‘decisions influence the environment with which the system interacts, be it in a physical or digital dimension.’¹³² The physicality of AI features prominently as among the very few systems that the proposed legislation bans altogether there are those that distort human behaviour ‘whereby physical or psychological harms are likely to occur.’¹³³ At the same time, the new law does not fully

framework for private remedies and enforcement’ (Matthias Leistner, ‘The Commission’s Vision for Europe’s Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a Critical Primer’ (2021) 16 JIPLP 778, 784) will be of paramount importance.

¹²⁵ On this point, it has been convincingly observed that this Act does not revolutionise the EU approach to digital regulation, but it significantly increases the procedural tools available for national and EU enforcement’ (Savin (n 102)).

¹²⁶ Jorge Morais Carvalho, Francisco Argáez Lima and Martim Farinha, ‘Introduction to the Digital Services Act, Content Moderation and Consumer Protection’ (2021) 3 Revista de Direito e Tecnologia 71, 101.

¹²⁷ See e.g. Feifei Shi and others, ‘Recent Progress on the Convergence of the Internet of Things and Artificial Intelligence’ (2020) 34 IEEE Network 8.

¹²⁸ The European Council has stated the objective that the EU becomes a global leader in the development of secure, trustworthy and ethical AI (European Council, *Special meeting of the European Council* (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, 6). As noted by Natali Helberger and Nicholas Diakopoulos, ‘The European AI Act and How It Matters for Research into AI in Media and Journalism’ [2022] Digital Journalism 1, this is ‘one of the first attempts worldwide to cut through an increasingly opaque jungle of private and public ethical guidelines in order to formulate binding regulatory standards for what exactly responsible and human-centric AI must mean.’

¹²⁹ The text I have analysed is the European Commission’s initial proposal, available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206>> accessed 11 October 2022. It is most likely that the final text will be significantly different, as the current heated debate around facial recognition suggests (Luca Bertuzzi, ‘AI Act: EU Parliament’s Discussions Heat up over Facial Recognition, Scope’ (*Euractiv*, 6 October 2022) <<https://www.euractiv.com/section/digital/news/ai-act-eu-parliaments-discussions-heat-up-over-facial-recognition-scope/>> accessed 11 October 2022). This should not come as a surprise; indeed, it had already been predicted that the definitions set forth in the AI Act would hamper its objectives (Jan Czarnocki, ‘Will New Definitions of Emotion Recognition and Biometric Data Hamper the Objectives of the Proposed AI Act?’, *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)* (IEEE 2021) 1).

¹³⁰ Draft AI Act, art 2(1). The proposed regulation will not apply to US providers of AI systems if they are used or developed exclusively for military purposes, and in the context of international agreements for law enforcement and judicial cooperation with the EU or a Member State (see art 2(3) and (4)).

¹³¹ Draft AI Act, recital 6. Italics added.

¹³² Draft AI Act, recital 6.

¹³³ Draft AI Act, recital 16, which is an interpretive aid for art 5(1)(a) and (b).

appreciate that the IoT contributes to overcoming of the physical-digital dichotomy. Indeed, it introduces stringer rules for AI that is deployed in publicly accessible spaces and it explicitly limits these to physical spaces.¹³⁴

The core of the AI Act is the regulation of high-risk systems, which are not forbidden per se (e.g. government-run social scoring)¹³⁵ rather they become subject to specific legal requirements.¹³⁶ High-risk systems range from automated CV sifting through real-time biometric identification to automated student assessment systems.¹³⁷ The providers of these systems have to meet a number of obligations e.g. to put in place quality management systems, to undergo conformity assessment procedures, and affix CE marking.¹³⁸

In critically assessing whether the AI Act can counter smart monopolies, the new transparency obligations would *prima facie* constitute a natural starting point.¹³⁹ The key principle here is that the system must be designed and developed in a way that ensures that its ‘operation is sufficiently transparent to enable users to interpret the system’s output and use it appropriately.’¹⁴⁰ This in part builds on the debate around a right to an explanation of solely automated decisions under the GDPR,¹⁴¹ but ignores that often the developers themselves are unable to interpret the outputs of their AI systems.¹⁴² Additionally, the provision introduces a narrow concept of transparency; indeed, it mandates only an ‘appropriate type and degree of transparency’¹⁴³ and only for the limited purposes of achieving compliance with the other obligations of the Act.¹⁴⁴ As opposed to embracing an ethos of openness,¹⁴⁵ transparency appears to be seen as a meta-principle that reiterates the otherwise obvious concept that AI providers should open themselves to some degree of scrutiny in the event of non-compliance. Even when the provision requires that information be provided about the datasets used, it merely asks AI providers to communicate information about the data (not the data itself), only in the context of the explanation of the characteristics, capabilities, and limitations of the system, and with the possibility to opt-out of the requirement ‘when appropriate.’¹⁴⁶

¹³⁴ Draft AI Act, art 3(39); recital 9.

¹³⁵ This is used as the chief example of altogether banned AI system (as seen as creating an unacceptable risk for EU citizens) and, professedly, key differentiator to systems ‘used in China’ (‘What is the EU AI Act?’ (Artificial Intelligence Act) <<https://artificialintelligenceact.eu/>> accessed 11 October 2022. In fact, not all such social scoring systems are banned. They are only if they lead to the detrimental or unfavourable treatment of individuals or groups: (a) in social contexts which are unrelated to the contexts in which the data was originally generated or collected, or (b) if unjustified or disproportionate to their social behaviour or its gravity (Draft AI Act, art 5(1)(c)).

¹³⁶ Draft AI Act, Title III.

¹³⁷ See Annex III to the Draft AI Act, points 1, 3(b), and 4(a).

¹³⁸ Draft AI Act, art 16.

¹³⁹ Draft AI Act, art 52.

¹⁴⁰ Draft AI Act, art 13(1).

¹⁴¹ See inter alia Margot E Kaminski, ‘The Right to Explanation, Explained’ (2019) 34 Berkeley Tech. LJ 189.

¹⁴² Legal informatics studies are attempting to find ways to design AI-Act-compliant systems and it seems clear that the approaches currently in use are not fit for purpose. For example, Francesco Sovrano and others, ‘Metrics, Explainability and the European AI Act Proposal’ (2022) 5 J 126 have looked at explainability metrics and underlined the limited extent to which existing metrics meet the new requirements; instead, they argue that ‘metrics to measure the kind of explainability endorsed by the proposed AI Act shall be risk-focused, model-agnostic, goal-aware, intelligible, and accessible’ (ibid 138)

¹⁴³ Draft AI Act, art 13(1).

¹⁴⁴ A problematic aspect is the reference to only the obligations set forth in Chapter 3 of the Act, thus not covering the other obligations introduced in other parts of the instrument e.g. cybersecurity requirements under Chapter 2.

¹⁴⁵ This can be easily contrasted with the principle of good faith in consumer contracts, that mandates ‘fair and open dealing’ (*The Director General of Fair Trading v First National Bank plc* [2001] UKHL 52 [17] per Lord Bingham of Cornhill).

¹⁴⁶ Draft AI Act, art 13(3)(b)(v).

A separate Title is dedicated to ‘Transparency Obligations for Certain AI Systems’ and it contains only one provision.¹⁴⁷ One would therefore be entitled to expect that the latter contains a meaningful regulation of transparency of AI systems. On closer inspection, however, the relevant obligations are rather limited and the mostly apply to bots as virtual assistants and the like. Indeed, this provision merely requires that providers of AI systems interacting with human beings inform the latter that they are interacting with an artificial agent.¹⁴⁸ Specific, albeit not dissimilar, rules are set forth with regard to emotion recognition systems (that have to ‘inform of the operation of the system the person exposed’¹⁴⁹), deep fakes (that ‘shall disclose that the content has been artificially generated or manipulated’¹⁵⁰). It is rather disappointing that this is the very limited meaning of ‘transparency’ in the AI Act, especially given the professed awareness that the exercise of fundamental rights ‘could be hampered [...] where [high-risk] AI systems are not sufficiently transparent.’¹⁵¹ Overall, these findings are in line with previous research noting that the transparency provisions ‘either add little to existing law or raise more questions than answers when their implications are considered.’¹⁵²

This notwithstanding, another provision may play a role in countering smart data enclosures by forcing providers of AI systems, including IoT systems embedding AI, to be more transparent. Interestingly, here the law provides a power to access data, rather than a right or a duty. Indeed, Article 64 states that market surveillance authorities¹⁵³ shall be ‘granted full access to the training, validation and testing datasets’¹⁵⁴ through APIs or other technical means allowing remote access. Full access to datasets is crucial to overcome data enclosures and, positively, this appears to be an absolute power, i.e. one that AI providers cannot object to. This can be inferred by the fact that, in introducing a complementary power (in addition to the access to the training datasets), it subjects it to a proviso. Notably, market surveillance authorities shall be granted access to the source code of the AI system, but only ‘where necessary’¹⁵⁵ in the context of the conformity assessment of high-risk systems, and only ‘upon a reasoned request.’¹⁵⁶ A contrario, AI providers will not be able to deny the requests to access

¹⁴⁷ Draft AI Act, Title IV.

¹⁴⁸ Draft AI Act, art 52(1), which comes with the caveat that the obligation will not apply in the event that the use of the bot was authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

¹⁴⁹ Draft AI Act, art 52(2).

¹⁵⁰ Draft AI Act, art 52(3). This provision contains the precision that the obligation will not apply to the use of deepfakes that is (i) authorised by law to detect, prevent, investigate and prosecute criminal offences, or (ii) necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences.

¹⁵¹ Draft AI Act, recital 38.

¹⁵² Michael Veale and Frederik Zuiderveen Borgesius, ‘Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach’ (2021) 22 *Computer Law Review International* 97, para 108.

¹⁵³ This is defined by reference to the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L 169/1. Even after Brexit, the EU legislative framework for manufactured goods continues to apply in Northern Ireland under the Ireland/Northern Ireland Protocol.. Article 10 of the Regulation requires a Single Liaison Office to be established to represent the coordinated position of domestic market surveillance authorities; in the UK, this is the Office for Product Safety and Standards. See Office for Product Safety and Standards, ‘EU Regulation 2019/1020 on Market Surveillance and Compliance of Products. Guidance’ (*Gov.UK*, 11 June 2021) <<https://www.gov.uk/government/publications/eu-regulation-20191020-on-market-surveillance-and-compliance-of-products>> accessed 12 October 2022. The attribution of such wide powers to market surveillance authorities should be accompanied by clear independence guarantees, as underlined by Veale and Zuiderveen Borgesius (n 151) para 102.

¹⁵⁴ Draft AI Act, art 64(1).

¹⁵⁵ Draft AI Act, art 64(2).

¹⁵⁶ Draft AI Act, art 64(2).

the training, validation, and testing datasets on grounds of lack of necessity or insufficient justification. This power is pivotal to open up AI's black box and is therefore regrettable that it only rests with market surveillance authorities, especially as it would be of vital importance to exercise the fundamental rights to an effective remedy¹⁵⁷ and to a fair trial¹⁵⁸ – to which the AI Act pays lip service¹⁵⁹ – in the context of litigation between private parties.¹⁶⁰ The regulatory role of these authorities is part of a wider problem of the AI Act. Indeed, it has been noted that this bold interpretive expansion of regulation by market surveillance authorities visibly 'underestimates how different regulating users will be'¹⁶¹ from regulating economic operators, that are the traditional target of this type of regulation (e.g. in the context of product safety).

The statement that the power to access training, validation, and testing datasets is absolute – and therefore IP considerations should not trump it – must be tested against the confidentiality provisions in the AI Act. Article 64 itself mentions confidentiality solely as a limitation to the use (not to the access to) of 'any documentation created or maintained'¹⁶² by AI providers to comply with the Act. It does not apply to access to the data, but simply to the access to documentation e.g. the technical documentation that must be drawn up before the system is placed on the market or put into service.¹⁶³ As this provision does not apply to data – and, importantly, it only applies to national authorities enforcing EU fundamental rights, as opposed to market surveillance authorities – then the argument could be put forward that under this *lex specialis* AI providers cannot oppose market surveillance authorities' access to their datasets on grounds of IP. If we do not accept that the confidentiality paragraph in Article 64 is a *lex specialis* that prevails over the horizontal confidentiality requirements set forth in Article 70, then we need to move on to analyse the latter to critically assess whether it can be relied upon to oppose the power to access the datasets. Article 70 does state that the competent authorities shall respect the 'confidentiality of information and data'¹⁶⁴ so as to protect IPRs, confidential information, and trade secrets. However, it does not give AI providers carte blanche to enclose their data when confronted with requests from market surveillance authorities. Indeed, Article 70 requires that the relevant authorities 'respect the confidentiality of information and *data obtained* in carrying out their tasks and activities,'¹⁶⁵ which means that AI providers must grant access to all data, safe in the knowledge that, once obtained, the data will be handled in compliance with confidentiality and IP law. Additionally, an express counter-limitation is identified in the Trade Secrets Directive, whereby the unauthorised acquisition, use or disclosure of trade secrets is lawful if it is done in the exercise of freedom of expression and information (which as we said include the right both to impart and access information).¹⁶⁶ In other words, market surveillance authorities have an absolute power to access the datasets at issue, but the use – and exchange with other authorities – of the relevant data is accompanied

¹⁵⁷ Charter of Fundamental Rights of the European Union, art 47(1); European Convention on Human Rights, art 13.

¹⁵⁸ Charter of Fundamental Rights of the European Union, art 47(2); European Convention on Human Rights, art 6.

¹⁵⁹ Draft AI Act, preamble point 3.5, recital 28, 38, 40.

¹⁶⁰ In previous research, I argued that although in most instances consumers will not need to access the training datasets, this access is pivotal to an effective defence (as *Loomis v Wisconsin*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017) proved). In this sense, Noto La Diega (n 112) para 69.

¹⁶¹ Veale and Zuiderveen Borgesius (n 151) para 101.

¹⁶² Draft AI Act, art 64(3).

¹⁶³ Draft AI Act, art 11.

¹⁶⁴ Draft AI Act, art 70(1).

¹⁶⁵ Draft AI Act, art 70(1); see also recital 83.

¹⁶⁶ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1, art 5(a).

by binding confidentiality obligations.¹⁶⁷ In conclusion, despite its shortcomings, the AI Act could provide a useful tool for market surveillance authorities to access smart data, and, correspondingly, a strong incentive for AI providers – including providers of IoT devices embedding AI – to avoid smart data enclosures. Nonetheless, the move away from access rights and access duties to power to access is open to criticism because it shifts the burden onto a small number of authorities that are under resourced and currently lacking the relevant expertise; conversely, a successful strategy to open up AI data should strengthen both private and private enforcement, as well as judicial and administrative redress.

6. Conclusion

As Europe starts embracing quantum computing¹⁶⁸ – with its potential to solve complex societal problems ranging from health through energy transition to climate justice – there can no longer be doubt that the big data generated by IoT systems must become accessible and smart data enclosures must end. Alongside data access rights, obligations, and powers to access the data generated by or through ‘Things’ abound in the latest EU attempts to regulate the emerging technologies. This is a welcome step ahead in terms of moving away from single-minded rights-based approaches and previous debates on data ownership. The framework and the surrounding discussion are now centred on techno-legal ways to gain control over data through duty-based, platform-targeted, public-enforcement-focused regulatory approaches. However, the tensions between data openness and propertisation has not been fully resolved yet. The recent proposed or adopted legislative instruments tend to contain safeguard clauses to protect the proprietary interests of smart data holders. There is the risk that the legislative statements focused on the concept of striking a balance between openness and IP – while justifiable in principle – end up being de facto abused by the most powerful actors of the IoT to cement and even strengthen their data enclosures. While IP lawyers have always been fond of the concept of ‘balance’, the time has come to accept that other analytical (and operational) tools may be more appropriate; for example, we may need to accept that there is an unresolvable conflict between certain private and public interests and that a battle, rather than a balance, is needed. In this sense, although currently isolated in the context of EU data governance laws, the approach of the Digital Markets Act – that does not sacrifice openness on the altar of a balance with IP – ought to be regarded as best practice. As I finalise this chapter, the EU has just published an AI Directive¹⁶⁹ dealing with liability for AI-generated harms, and a new Product Liability Directive. In both data access features prominently¹⁷⁰ and both include IP-related safeguard clauses,¹⁷¹ which will have to be the subject of future research.

In conclusion, the EU lawmaker should leave it to the already hypertrophic IP framework to protect the proprietary interests of IoT big tech. EU data governance laws should be focused on creating the conditions for unencumbered data flow; and IP proviso are likely to be exploited to effectively sterilise the ethos of openness of the new laws. Their focus should be on providing a combination of access rights, duties, and powers, accompanied by public and private enforcement, judicial and administrative redress, and effective controls over the role of

¹⁶⁷ See also Draft AI Act, arts 30(6) and 33(6).

¹⁶⁸ For example, in October 2022 the European High-Performance Computing Joint Undertaking announced the deployment of the first European quantum computers, which will be integrated into existing supercomputers and will be part of a wide network across the EU. See ‘Selection of Six Sites to Host the First European Quantum Computers’ (*EuroHPC*, 4 October 2022) <https://eurohpc-ju.europa.eu/selection-six-sites-host-first-european-quantum-computers-2022-10-04_en> accessed 11 October 2022.

¹⁶⁹ Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM(2022) 496 final).

¹⁷⁰ AI Directive, art 3; Second Product Liability Directive, art 8.

¹⁷¹ AI Directive, art 3(4); Second Product Liability Directive, art 8(3).

private players in rule-setting and enforcing. Too much is at stake: EU's competitiveness, its role as digital regulation leader, and its contribution to tackling the big societal challenges of our time.