Rachel Masterton*

International Cooperation: Expanding Capacity, Amplifying Impact**

The processing of personal data is often on a global scale with global impacts. Regulation, on the other hand, has been constructed according to geographical boundaries. International cooperation can be the resolution to those geographical differences and by engaging with the four modalities of regulation identified by Lawrence Lessig[1] in his 'Pathetic Dot Model' this cooperation can serve to expand the capacity and amplify the impact of data protection and privacy authorities.

Keywords: *Lessig, Pathetic Dot Model, data protection, international cooperation, regulation, privacy.*

1. Introduction

Personal data has become a global business stretching beyond geographical boundaries. The regulation of those entities making money from personal data, however, remains firmly anchored to these traditional, jurisdictional boundaries. Even when legislation is shared by a number of countries, such as the European Union's General Data Protection Regulation[2], each jurisdiction has their own body tasked with regulation and enforcement, in some cases, several bodies.

International cooperation by data protection authorities is, therefore, vital to knit together disparate legal frameworks for a global response to global problems. However, there is more to be gained from international cooperation than simply smoothing out legal differences.

This paper seeks to explore the four modalities of regulation, as proposed by Lawrence Lessig[3] - law, societal norms, market and architecture - and, using case

* LLM, Deputy Data Protection Commissioner, Guernsey Data Protection Authority.

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

[1] *Lessig L., Code Version 2.0* (Basic Books 2006).

[2] 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 [2016] OJ L119.

[3] *Lessig L.*, Code and the Other Laws of Cyberspace, Basic Books, 1999.

studies, show how these modalities, when combined with international cooperation, can help data protection authorities expand their capacity and amplify their impact.

2. Understanding Lessig's Modalities of Regulation

Lawrence Lessig first wrote about the four modalities of regulation, also known as the 'Pathetic Dot Model' in his book 'Code and the Laws of Cyberspace'. He postulated that an entity ('the dot') is subject to four different forces that control or regulate its behaviour. These four forces are law, social norms, the market, and architecture, in Lessig's case, 'the code' underpinning cyberspace.

Law provides the rules that the State wants to control activity. It codifies what is right and what is wrong and provides mechanisms to judge the legality of activity and to sanction that which is deemed wrong. This informs the dot what is legal and what could happen if it does not follow the law.

Social norms are the unwritten rules of behaviour that operate within a society. They are not set by the State but rather by those people in the society to whom the social norms relate. Unless there is a crossover with a piece of legislation there are likely no formal sanctions imposed if a social norm is broken or ignored. However, the society itself will often act as the judge of the behaviour and make its feelings known in other ways. In days past, this would be by word of mouth. Now, in this digital age, social norms are the reason user-generated review platforms such as TripAdvisor hold so much power. They represent not what behaviour is legal or illegal but rather how someone felt the behaviour of a business met their expectations and a societal view of good or bad.

The market in which the dot operates has long been a way in which activity is regulated. Markets set prices based on supply and demand. A business can charge more for a rare product than it could for a more common one, even where a dispassionate view would suggest they are of the same value. Markets can also determine what an acceptable product or service is and those not meeting that standard can suffer by comparison.

Architecture relates to the physical and situational factors that act to constrain the dot. As Lessig puts it, architecture is "the way the world is, or the ways specific aspects of it are". Architecture shapes human behaviour, for example, the layout of a town controls or constrains how people interact with it. A person needs to follow the roads and move past the building rather than heading 'as the crow flies'.

The book Lessig wrote deals primarily with regulation of the cyberspace and was written in response to a commonly held belief that cyberspace could not be regulated. This therefore has some resonance in the data protection world and will be explored further later in this paper. However, it is clear from looking at the model, that the four modalities of regulation are not exclusive to the online world and can be considered in relation to the regulation of behaviour in other arenas. Lessig argues that these four modalities act on the dot, each individually but often simultaneously, to a greater or

lesser extent depending on the circumstance and that leveraging all modalities will have a greater impact than focusing solely on one.

As an example, one need look no further than the global initiative to combat climate change. Treaties have been signed[4] and legislation has been enacted[5] to curb emissions and remove some of the more harmful contributors of 'greenhouse gases' – regulation by law. Schools, colleges and third-sector bodies are educating people as to the difference they can make by changing behaviour and encouraging change in others – regulation by societal norms. Companies are making shifts in their production methods and creating new 'greener' products, shifting the market share away from more established but more harmful practises – regulation by the market. In addition, global reserves of non-renewable and harmful energy sources are depleting, forcing the world to think about alternative energy – regulation by architecture.

In the middle of those four modalities is the dot. Whether the dot in this example represents a person or a company, all four modalities are working on it, applying their pressure in their different ways, but all regulating the behaviour of the dot.

3. The Landscape of International Data Protection Regulation

As of 2 July 2025, 79% of the world's countries had some form of data protection or privacy legislation, according to statistics published by the United Nations Trade and Development ('UNCTAD')[6], with a further 3% of countries having draft legislation. Whilst these laws provide frameworks for the obtaining, use and storage of personal data, there is no overarching legal instrument that all 80% have signed up to and organisations with activities in several different jurisdictions will often find differences in the requirements and expectations of the regulators created by those laws. In some cases, such as in the United States of America, legislation is State-focused[7] or sector-focused[8] meaning different rules in different circumstances, even within the same country.

That said, there are two significant legal frameworks, the European Union's General Data Protection Regulations and the Council of Europe's Convention 108[9], that form the basis of many of the world's data protection and privacy legislation. There are many commonalities between these two frameworks. Both are built on

[4] Paris Agreement to the United Nations Framework Convention on Climate Change, adopted 12 December 2015, T.I.A.S. No. 16-110.

[5] Climate Change Act 2008 (c. 27).

[6] *UN Trade & Development*, 'Data Protection and Privacy Legislation Worldwide' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

[7] The California Privacy Rights Act of 2020, implemented & enforced by the California Privacy Protection Agency <https://cppa.ca.gov/about_us/>.

[8] Health Insurance Portability and Accountability Act of 1996 (HIPAA) <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>.

[9] *Council of Europe*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (opened for signature 28 January 1981).

fundamental principles; the processing of personal data must be lawful, fair and transparent, collected for specified legitimate purposes and not used beyond those purposes. Both frameworks provide individuals with rights over their personal data. These include the right to access personal data, to request rectification and erasure and the right to object to processing.

Both frameworks place an emphasis on accountability, requiring those using personal data to implement appropriate measures to ensure compliance and to be able to demonstrate that compliance. In addition, as both are designed to apply across jurisdictions, both frameworks contain provisions for international data transfers, to assist business in operating and to ensure that the safeguards provided by the frameworks travel with the personal data.

However, despite the broad similarities, even these two frameworks have significant differences. The GDPR is an EU regulation and as such is directly applicable in EU Member States. It is also detailed and prescriptive, leading to a robust framework that is the same across the EU and EEA. The GDPR provides a mechanism under which third countries can apply to have their own data protection legislation and regulatory frameworks determined as adequate. This assessment of the third country as essentially equivalent to the GDPR provides for the free-flow of personal data between EU and adequate jurisdictions without the additional safeguards a transfer outside the EU's boundaries would usually require. To date, 16 such decisions have been made.

The Convention 108 is, in contrast, an international treaty and whilst laying out guiding principles, is in no way as prescriptive as the GDPR. Signatory jurisdictions are required to enact their own domestic legal instruments to implement the principles of the Convention. As such, whilst its reach is wider than that of the GDPR, there can be differences in implementation across the 55 jurisdictions that have adopted it, 47 Member States of the Council of Europe and five non-European countries[10].

Whilst legislation may differ across the globe, cooperation between the regulators of different jurisdictions that have similar aims has long been an important part of the regulatory stage. In 1979, the first International Conference of Data Protection and Privacy Commissioners was held in Bonn, Germany[11]. Held in a different country each year (except for two 'at your desk' events during the COVID-19 pandemic) and hosted by a local data protection or privacy regulator, this conference has grown both in size and remit. Rebadged as Global Privacy Assembly[12] ("the GPA") and guided by an Executive Committee, supported by a secretariat, the GPA embraces the following as its vision: Consolidate the Global Privacy Assembly's leadership on personal data protection and privacy, maximizing its voice and influence across geographic and linguistic networks and strengthening the enforcement capacities of

[10] Council of Europe 'Chart of signatures and ratifications of Treaty 108'. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

[11] Global Privacy Assembly 'History of the Assembly' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.

[12] Global Privacy Assembly <https://globalprivacyassembly.org/>.

authorities to move towards a higher level of global data protection and privacy that ensures effective protection of data subjects.[13]

As well as providing an annual forum for discussion between its over 130 members and observers, the GPA has adopted a plan[14] that articulates its strategic aims. These are focused around achieving a higher level of global data protection and privacy, maximising the voice and influence of the GPA and its members and strengthening enforcement capacities. To deliver on these aims, the GPA has a number of working groups[15] that bring together member data protection and privacy authorities that work in collaboration to achieve more than they could alone.

Of particular relevance to the theme of this paper is the International Enforcement and Cooperation Working Group[16]. Established as a permanent working group in 2019, the IEWG has the remit to "lay the foundations for the IEWG and GPA to facilitate practical enforcement cooperation"[17] with a particular focus on global issues that could affect people's data protection and privacy rights. It also seeks to develop and promote practical tools to assist international enforcement cooperation and to foster lines of communication with other relevant groups and privacy bodies to "coordinate and leverage opportunities"[18]. One tool supported by the IEWG is the Enforcement Cooperation Handbook[19] (the Handbook) that lays out ways in which authorities can work together to achieve common goals. The work of the IEWG and the Handbook will be discussed in the next section of this paper.

The Global Privacy Enforcement Network[20] (GPEN) was created in response to the OECD's Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy[21]. Paragraph 21 of that document called for the "establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders" to discuss cooperation and share best practices in dealing with cross-border issues. One of GPEN's headline initiatives is the annual 'Sweep', a mechanism "aimed at increasing awareness of privacy rights and responsibilities, encouraging compliance with privacy legislation, and enhancing cooperation between

[13] Global Privacy Assembly 'Mission and Vision' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/>.
[14] Global Privacy Assembly 'Strategic Plan 2023 – 2025' <https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf>.
[15] Global Privacy Assembly 'Working Group Reports' <https://globalprivacyassembly.org/document-archive/working-group-reports/>.
[16] Global Privacy Assembly 'International Enforcement Working Group Report – July 2024' <https://globalprivacyassembly.org/wp-content/uploads/2024/11/9.-IEWG-GPA-Annual-Report-2024.pdf>.
[17] Ibid.
[18] Ibid.
[19] Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.
[20] Global Privacy Enforcement Network <https://privacyenforcement.net/content/home-public>.
[21] OECD, Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352.

international privacy enforcement authorities"[22]. Part of GPEN's Action Plan is to build a "network of networks"[23] comprising other privacy and data protection networks as well as other regulatory networks with interests that intersect with those of the GPEN's. One example is the 2024 Sweep in which GPEN teamed up with the International Consumer Protection Enforcement Network[24] to look at deceptive design patterns in websites and applications[25]. This is discussed in more detail in the next section as an example of the benefit of cooperation.

4. Applying the Pathetic Dot Model to International Data Protection Cooperation

When considering the Lessig Pathetic Dot Model in the context of international regulatory cooperation, it is easy to see the relevance of the law modality. All data protection and privacy regulators are creatures of law; created and given their powers and duties by legislation. Law sets out the requirements for organisations when processing personal data and the rights of individuals. Law provides the breach reporting and complaint mechanisms, frameworks for how regulators are required to handle such matters and the sanctions that can be issued for wrongdoing. As Lessig identified, law pushes regulated entities to behave as the State requires and will penalise those that do not comply.

As creatures of law in a digital world that knows no boundaries, it is perhaps inevitable that investigations into large data breaches is a focus for cooperation. Big breaches by big companies often require a big response, and one data protection authority may see benefits in joining forces with a like-minded regulator from another jurisdiction.

A recent example of international cooperation was the joint investigation into a breach by genetic testing company 23andMe, conducted by the Office of the Privacy Commissioner of Canada (the OPC)[26] and the UK's Information Commissioner[27] (the ICO). This collaboration is perhaps not surprising, given that both regulators were key contributors to the Enforcement Cooperation Handbook[28] that outlines how, amongst other activities, joint investigations can be conducted.

---

[22] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

[23] Global Privacy Enforcement Network 'Action Plan for the Global Privacy Enforcement Network (GPEN)' <https://privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>.

[24] ICPEN <https://www.icpen.org/>.

[25] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

[26] Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.

[27] ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.

[28] Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.

In October 2023, an individual claimed that they had breached 23andMe's systems and had copies of personal data that they were offering for sale. Later that month, the OPC and the ICO were advised by 23andMe that a number of affected individuals came from their jurisdictions.

Whilst the two jurisdictions had their own legislation, there were sufficient similarities to make a joint investigation viable, made possible by a Memorandum of Understanding between the two regulators, "pursuant to section 23.1 of PIPEDA[29] and Article 50 UK GDPR". The outcome of the joint investigation, issued in June 2025, was the finding of breaches under both PIPEDA and the UK GDP that during the investigation 23andMe had addressed such that the issues were deemed resolved[30]. However, in an example of a difference between legislative frameworks, the ICO had the power to fine and issued a monetary penalty of £2,310,000[31] on top of the finding.

Leveraging the law modality of the Pathetic Dot Model seems natural for data protection and privacy regulators and cooperation with international counterparts can expand a regulator's capacity and amplify their impact. However, investigations can be lengthy and resource intensive and are focused only on the behaviour of one organisation. There can be no doubt of the effectiveness of an investigation and sanction on 23andMe. During the investigation, whilst under the microscope of two regulators, the company addressed its shortcomings and improved its compliance. But it can be difficult to judge the impact of that case on other organisations, whether the lessons learnt by 23andMe are acted on by other organisations and whether the fine issued acts as a deterrent. It is with this in mind that the other three modalities of the Pathetic Dot Model should be considered and how, through international cooperation, these can be leveraged by data protection and privacy authorities to regulate behaviour.

To demonstrate this, this paper will discuss two examples of international cooperation used by the Office of the Data Protection Authority of Guernsey[32] (the ODPA). As one of the smallest data protection authorities in the world[33], it has looked to international cooperation to both provide additional capacity for action and to increase the impact of its actions. As an international finance centre, the Bailiwick of Guernsey[34] (the Bailiwick) is already punching above its weight, and a robust data protection regime can help secure that position. Further, as technology does not respect geographical boundaries, the Bailiwick's citizens face the same data protection

[29] Personal Information Protection and Electronic Documents Act (PIPEDA).
[30] Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.
[31] ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.
[32] formally known in the Data Protection (Bailiwick of Guernsey) Law, 2017 as the Data Protection Authority
[33] 14 staff at time of writing.
[34] The Bailiwick of Guernsey comprises the islands of Guernsey, Alderney, Sark and Herm and is located in the English Channel. As a British Crown Dependency, it is a self-governing jurisdiction, with allegiance to the British Crown.

and privacy problems as much larger jurisdictions and deserve a regulator that can represent them on the international stage whilst adding value and benefits locally.

In 2024, the ODPA became a signatory to the joint statement on data scraping and the protection of privacy[35], an initiative of the GPA's IEWG. This joint statement, endorsed by 14 international data protection authorities, outlined the privacy risks from data scraping, how social media companies and operators of other websites could protect users' data, and the actions individuals could take to protect themselves. As the Bailiwick's Commissioner, Brent Homan, said, "Data-scraping poses a global risk that calls for a global response [...] In joining forces with our international data protection partners we are setting out key global expectations for social media companies towards ensuring adequate safeguards to combat non-authorised scraping"[36].

Following the issuance of the joint statement in August 2023, the signatories engaged with the leading social media companies to understand the technical challenges they faced in combatting unlawful data scraping and the actions they were taking. The virtual meetings allowed the ODPA to question these companies directly, something that would have been almost impossible without the combined weight of the other regulators involved in this initiative. Signatories also met with representatives of the Mitigating Unauthorized Scraping Alliance[37] (MUSA), a body that brings together "industry leaders to protect data from unauthorized scraping and misuse"[38].

The information gleaned in these important meetings led to the publication of a concluding joint statement that outlined additional expectations including that the training of AI large language models should be cognisant of data protection and privacy legislation, that safeguarding measures deployed to combat unlawful scraping should be reviewed regularly to keep pace with advancing technology and that data scraping permissible for commercial or societally beneficial purposes must be done lawfully[39].

Considering this initiative in terms of the Pathetic Dot Model, the law modality is at play as the basis for the expectations laid out in the joint statements were the legal obligations placed on organisations when processing personal data. However, this was not the only modality in play. By engaging with leading social media companies, the signatories were asking the market to apply its own pressure on entities to behave in an acceptable manner.

Whether it be by using their own compliant practices as a competitive advantage, appealing to privacy-conscious individuals or by calling out bad practice, getting the market or industry to act as a gatekeeper can be the extra push outliers need. This leveraging of the market was further demonstrated by the engagement with MUSA.

[35] ODPA 'ODPA joins international efforts to prevent unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=5a294e41-9eea-ee11-a204-6045bd8c5a56>.
[36] Ibid.
[37] MUSA <https://antiscrapingalliance.org/>.
[38] Ibid.
[39] ODPA 'Guernsey joins global partners to combat unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=f5ed30b6-3595-ef11-8a69-6045bdf2d3b5>.

This body was already in existence and seeking to promote good practice whilst raising public awareness. It was of benefit to MUSA to be seen to be engaging with regulators but, in turn, it was another opportunity for regulators to move the market modality, to the benefit of individuals and compliant companies alike.

In addition to making use of the market modality, through press releases and speaking engagements, the ODPA was able to leverage the societal norms modality. It provided opportunities to educate the public as to how their personal data could be used in a way they were neither expecting nor happy with. This empowers them to take steps to protect themselves, either by limiting the data they share with web-based platforms or by making choices based on how responsible the operator may be. By challenging the idea that 'that's the way it's always been and there is nothing I can do about it', external communications may activate the public to alter the societal norm and thus exert pressure on regulated entities.

Anecdotal evidence suggests that following ODPA press releases, data scraping became a topic of conversation between individuals and across boardroom tables showing that engaging with other modalities can spread a message and influence a narrative.

A further example of the power of international cooperation was the 2024 GPEN Sweep[40]. The topic was deceptive design practices or 'dark patterns', those aspects of website and app design that pushes the least privacy-friendly option to the benefit of the company and detriment of the individual. The Sweep saw GPEN join forces with the International Consumer Protection Enforcement Network[41], its consumer protection counterpart, to review websites and apps for indicators of dark patterns.

Over a thousand websites and apps were 'swept' as part of this initiative, by 26 privacy enforcement authorities and 27 ICPEN authorities making the Sweep "the most extensive example of cross-regulatory cooperation between privacy and consumer protection authorities, to date"[42]. Overall, 97% of websites and apps reviewed showed at least one indicator of deceptive design patterns[43].

One prominent industry in the Bailiwick of Guernsey is egambling. This sector is subject to regulation by the Alderney Gambling Control Commission[44] (the AGCC). Given the prevalence of problem gambling and the vulnerability of some users of egambling websites and apps, the ODPA focused its Sweep on those companies licensed by, and provided its results to, the AGCC. At the beginning of February 2024, 19 companies were 'swept' and each was found to have at least one indicator of

[40] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>
[41] ICPEN <https://www.icpen.org/>.
[42] Global Privacy Enforcement Network 'GPEN Sweep 2024: "Deceptive Design Patterns" Report' <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf>.
[43] Ibid.
[44] Alderney Gambling Control Commission <https://www.gamblingcontrol.org/>.

deceptive design practices with particular concerns about the transparency of processing[45].

As a result of the Sweep, the ODPA wrote to each company swept outlining its concerns both across the industry as a whole and specifically in relation to their own websites and apps. In less than three months, the ODPA received commitments from 78% of those companies to improve their practices and specifically address the concerns[46]. In one case, the data protection officer welcomed the ODPA's correspondence as it restated concerns they had expressed previously internally and the ODPA's intervention helped them secure the change they were seeking.

In an example of the market and societal norms modalities in action, by the end of 2024, all companies had committed to improvements. The last company confirmed its commitment following an industry conference at which the ODPA's Commissioner expressed his appreciation to those companies that had committed to change. It realised that it was vulnerable to being cast in a poor light by its industry counterparts (market modality) and that users were expecting better (societal norms modality). Whether it was a case of self-interest or a genuine desire to improve, the ultimate outcome was a remarkable 100% commitment to improve, an action that would have taken many years if tackled through investigations.

Turning to the fourth modality – architecture - with technology moving apace and providing its own behavioural constraints whilst embracing innovation the clearer regulators are about their expectations and the more consistent those expectations are across the globe, the more developers can build these expectations into their products. In the run up to the GDPR coming into force, organisations' inboxes were flooded with adverts for technical solutions for GDPR. Some were more legitimate than others but it shows that an emphasis on accountability and privacy by design drove technological developments.

Activities such as the GPEN Sweep or the joint data scraping statements set out expectations and requirements. The enthusiasm of developers to provide solutions for common problems that they can market as responding to regulators expectations can see the architecture modality applying its own pressure to the pathetic dot. Cooperation by regulators can see global technical solutions to global technical problems.

[45] ODPA 'ODPA examines Bailiwick's gambling sector for harmful privacy practices as part of global sweep' <https://www.odpa.gg/news/news-article/?id=baea8752-d03d-ef11-8409-7c1e5226329b>.

[46] ODPA 'Bailiwick's gambling sector pledges to make improvements after ODPA shares concerns of harmful privacy practices' <https://www.odpa.gg/news/news-article/?id=cd258672-9f79-ef11-a670-6045bd97f872>.

5. Conclusion

Lawrence Lessig's 'Pathetic Dot Model' shows that whilst data protection and privacy are legal constructs, the reality is that there is more than just the law that acts to regulate the behaviour of the entity, or dot, that is being regulated. Pressure, constraints and impetus can be applied as effectively through the societal norm, the market and the architecture with which the entity interacts and the four modalities can be harnessed to drive improvements to the benefit of all stakeholders.

Importantly, whilst this can be achieved by data protection and privacy regulators acting on their own, international cooperation can strengthen these modalities and seek to resolve the problems posed by differing legislative mechanisms. This paper also shows that international cooperation does not have to be in the form of resourcing intensive joint investigations to lead to a positive change. A clear, consistent position adopted by regulators from across the globe can have as much, if not more, impact on the entity as a hefty fine issued to a competitor.

International cooperation is an invaluable tool in a regulator's arsenal. Whether a large or small regulator, one with many years in the game or one just starting out, international cooperation can expand capacity and amplify impact.

Bibliography:

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 [2016] OJ L119.
2. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (opened for signature 28 January 1981).
3. Paris Agreement to the United Nations Framework Convention on Climate Change, adopted December 12, 2015, T.I.A.S. No. 16-1104.
4. Climate Change Act 2008 (c. 27).
5. *OECD,* Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352.
6. *Lessig L,* Code and the Other Laws of Cyberspace (Basic Books 1999).
7. *Lessig L,* Code Version 2.0 (Basic Books 2006).
8. Alderney Gambling Control Commission <https://www.gamblingcontrol.org/>.
9. BBC News 'GDPR: Are you ready for the EU's huge data privacy shake-up?' <https://www.bbc.co.uk/news/technology-43657546n>.
10. Council of Europe 'Chart of signatures and ratifications of Treaty 108' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

11. Global Privacy Assembly <https://globalprivacyassembly.org/>.
12. Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.
13. Global Privacy Assembly 'History of the Assembly' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.
14. Global Privacy Assembly 'International Enforcement Cooperation Working Group Report – July 2024' <https://globalprivacyassembly.org/wp-content/uploads/2024/11/9.-IEWG-GPA-Annual-Report-2024.pdf>.
15. Global Privacy Assembly 'Mission and Vision' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/>.
16. Global Privacy Assembly 'Strategic Plan 2023 – 2025' <https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf>.
17. Global Privacy Assembly 'Working Group Reports' <https://globalprivacyassembly.org/document-archive/working-group-reports/>.
18. Global Privacy Enforcement Network <https://privacyenforcement.net/content/home-public>.
19. Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.
20. Global Privacy Enforcement Network 'Action Plan for the Global Privacy Enforcement Network (GPEN)' <https://privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>.
21. Global Privacy Enforcement Network 'GPEN Sweep 2024: "Deceptive Design Patterns" Report' <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf>.
22. ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>
23. ICPEN <https://www.icpen.org/>.
24. MUSA <https://antiscrapingalliance.org/>.
25. ODPA 'Bailiwick's gambling sector pledges to make improvements after ODPA shares concerns of harmful privacy practices' <https://www.odpa.gg/news/news-article/?id=cd258672-9f79-ef11-a670-6045bd97f872>.

26. ODPA 'Blog: Dark patterns and the gambling industry' <https://www.odpa.gg/news/news-article/?id=dccb80cb-3156-ef11-bfe3-000d3a2d37f7>.
27. ODPA 'Guernsey joins global partners to combat unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=f5ed30b6-3595-ef11-8a69-6045bdf2d3b5>.
28. ODPA 'ODPA examines Bailiwick's gambling sector for harmful privacy practices as part of global sweep' <https://www.odpa.gg/news/news-article/?id=baea8752-d03d-ef11-8409-7c1e5226329b>.
29. ODPA 'ODPA joins international efforts to prevent unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=5a294e41-9eea-ee11-a204-6045bd8c5a56>
30. Office of the Privacy Commissioner of Canada, 'Concluding joint statement on data scraping and the protection of privacy' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2024/js-dc_20241028/>.
31. Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.
32. Office of the Privacy Commissioner of Canada, 'Joint statement on data scraping and the protection of privacy' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/js-dc_20230824/>.
33. UN Trade & Development, 'Data Protection and Privacy Legislation Worldwide' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.