Singapore Journal of Legal Studies
[2021] 19–38

ENFORCEMENT DESIGN FOR DATA PRIVACY: A COMPARATIVE STUDY

GEHAN **GUNASEKARA***

This article explores whether design of enforcement mechanisms in data privacy laws influences the types of privacy harms addressed by them through evaluating evidence of enforcement from four jurisdictions. It uses three of the foundational design principles identified by Cavoukian to examine if each category of data privacy (data quality, access rights, use, disclosure, security and so forth) should be addressed through enforcement tools suited to their characteristics. The evidence supports the need for proactive regulator-led enforcement, rather than reactive litigation by complainants in relation to some areas. Such enforcement also has an educative function aligning with the principle of transparency. Where full functionality necessitates mechanisms for individuals to litigate complaints, the research found that specialist tribunals were more sympathetic to complainants than were courts. It also discovered that litigation by individuals tended to be linked to disputes between the parties unrelated to privacy and addressed only harms that came to light through complainants' prior knowledge. Finally, the evidence from each jurisdiction studied provides useful lessons for other jurisdictions as to both the conduct targeted and the need for substantive rules such as erasure or the right to be forgotten.

I. INTRODUCTION

The concept of "Privacy by Design" has become something of a buzzword, especially following the coming into force of the European *General Data Protection Regulation* ("*GDPR*") .[1] It has undoubted relevance in the context of regulating phenomena such as Big Data.[2] Does the concept of design, however, apply also to the very architecture of regulation itself, especially the enforcement tools available, for information or data privacy?[3] Generally, design is aimed at improving privacy outcomes and not specifically enforcement outcomes.[4]

---

* Associate Professor in Commercial Law, University of Auckland. I am grateful for the assistance provided by Ravi Maharaj, whose summer research scholarship enabled this research to be undertaken.

1 European Commission, *Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ, L 119/1, art 25 [*GDPR*].

2 Eric Everson, "Privacy by Design: Taking Ctrl of Big Data" [2017] 65 Clev St L Rev 27.

3 This article will use the term "data privacy" instead of "information privacy" throughout.

4 See R Jason Cronk, *Strategic Privacy by Design* (Portsmouth: International Association of Privacy Professionals, 2018) at ch 1.

However, aspects of the concept first articulated by Ann Cavoukian[5] apply with equal cogency to the design of enforcement mechanisms for implementing data privacy norms. For example, the concept of being proactive rather than reactive (Principle 1) might apply where privacy authorities seek out weaknesses in organisations' practices before breaches occur. Full functionality (Principle 4) may apply to enforcement not being a zero-sum game with either litigation by individuals or solely regulator-led enforcement.[6] Visibility and transparency (Principle 6) clearly apply to the activities of privacy authorities themselves in their educative and enforcement roles. These three in particular, of Cavoukian's seven foundational principles, may be adapted in the enforcement arena.

This article therefore explores design from the standpoint of the effectiveness of the remedies available when data privacy lapses occur as well as the effectiveness of tools available to ensure compliance with data privacy laws proactively. It examines the data privacy regulatory frameworks of four jurisdictions—Australia, New Zealand, Hong Kong and the United Kingdom—through the documented outcomes achieved by them over a six-year period from 2013 until 2018. Materials examined include the annual reports of the supervisory authorities, and other output including investigative reports, enforceable undertakings, penalty notices and case law. All four jurisdictions share a common principles-based normative framework based on the Organisation for Economic Cooperation and Development ("OECD") model.[7] The United Kingdom, however, is the most aligned with latest normative developments, especially the *GDPR*.[8]

The premise of the research is that the law's design as regards enforcement affects the conduct targeted by the law. Hence, until recently, New Zealand relied on enforcement largely through the pursuit, by individuals, of their rights in a dedicated specialist tribunal.[9] The narrow focus on contravention of an individual's rights may often result in decisions based on technicalities such as whether a causative link between the conduct and harm existed and may lead to wider systemic problems at the organizational level being ignored.

Similarly, despite the increasing prevalence of breach notification laws worldwide, assessing the extent of harm in relation to privacy breaches has always been difficult. When an individual brings a claim concerning a specific breach, the harm tends to be in the nature of a loss of some benefit, humiliation or simply injury to feelings. The research reveals that a subjective element exists as to how this is assessed. Where

---

5 Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Ontario: IAPP, 2010), online: IAB.ORG (2009) <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>.

6 See *GDPR*, *supra* note 1, art 78, which details the full spectrum of rights including individual judicial remedies, as well as a right to a review of supervisory authorities' decisions employing terminology such as "Without prejudice to any other administrative or non-judicial remedy".

7 See OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL (as amended on 11 July 2013 by C(2013)79) (2013) [*OECD Guidelines*].

8 All the United Kingdom enforcement activities catalogued during the period of the study related to the *Data Protection Act 1998* (UK), c 29 [*UK Data Protection Act 1998*]; the *Data Protection Act 2018* (UK), c 12 [*UK Data Protection Act 2018*] came into force from 25 May 2018.

9 Gehan Gunasekara and Niveet Singh, "Upping the Ante: New Actors and the Evolving Nature of Privacy Act Jurisprudence in New Zealand" [2017] 48 VUWLR 441 [*Gunasekara and Singh*, "Upping the Ante"].

regulators seek to impose fines, on the other hand, this tends to be aimed at deterring conduct that has the potential to affect many individuals and is therefore proactive in its aims.

This study across jurisdictions reveals that where monetary penalties have been imposed following a breach these are invariably linked to related systemic lapses in other areas, including retention, storage and disposal of personal data, which were the underlying causes of the breach. There are parallels here with a fine imposed on a driver who causes an accident through speeding or carelessness—it is the speeding or careless behavior that is being punished, in addition to causing the accident itself.

Finally, the research highlights more fundamental architectural issues concerning the nature of data privacy principles and the need for additional principles. It will be seen, for example, that a substantial number of security breaches resulted from the retention of data when it was no longer required. This provides a cogent argument for the so-called "right to be forgotten" or right to erasure in the digital era. In addition, the lessons learned from regulators' investigative reports—such as determining when data is no longer required—are of wider relevance outside their jurisdictions and, it is argued, amount to a compelling source of data privacy jurisprudence of equal or greater weight to traditional legal sources.[10]

II. Methodology

The research for this article, conducted over the summer of 2018/2019, focused on four jurisdictions. Three of these—New Zealand, Australia and Hong Kong—are in the Asia-Pacific whilst the fourth, the United Kingdom, was added for comparative and benchmarking purposes. Although the substantive statutory underpinnings regarding data privacy in these jurisdictions were not the focus of the research, it was nonetheless impossible to ignore them completely. For example, comparisons as to areas of data privacy that were the subject of either complaint or investigation required reference to the data protection or privacy principles involved and some coalescing of these had to occur.[11]

Instead of concentrating on these differences, however, the research examined the documented outcomes, in the period from 2013 until 2018 inclusive, as to enforcement of data privacy norms across the jurisdictions. These consisted in the main of investigative reports, monetary penalty notices and litigation by individuals—whether before courts or specialist bodies (including data protection or privacy commissioners). Enforceable undertakings, enforcement notices and prosecutions were recorded but space does not allow their detailed separate treatment below. The data was obtained from a range of sources such as annual reports of the authorities themselves as well as from legal databases such as Westlaw International.

---

[10] See Daniel Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy" [2014] 114 Colum L Rev 583.

[11] For instance, data retention was treated differently across the jurisdictions, with some having a separate principle: see *Privacy Act 1993* (NZ), 1993/28, s 6, Principle 9 [*NZ Privacy Act 1993*]. Others include it as a standalone rule or within another principle such as data quality or access and correction: see *Personal Data (Privacy) Ordinance 1995* (HK), s 26 and Schedule 1, Principle 1 [*HK Personal Data Ordinance 1995*]; *Privacy Act 1988* (Cth), Schedule 1, Australian Privacy Principle 13 [*Australian Privacy Act 1988*].

The documented outcomes studied were primarily those where complaints were authoritatively resolved in the first instance or where other forms of authoritative enforcement or investigations were initiated. Further appeals and reviews of these instances were not addressed except in a few instances where the matters led to significant precedents or guidance from appellate or review bodies. In the United Kingdom, where the data privacy authority, the Information Commissioner, lacks a formal conciliatory role, litigation by individuals in courts of law to enforce their data privacy rights were substantially eclipsed by the Commissioner-led measures referred to above.[12]

Both Australia[13] and New Zealand[14] confer a formal conciliatory role, in relation to complaints, on their respective data privacy authorities. Australia, in addition, confers a formal adjudicative role to its authority, the Australian Information Commissioner, to make determinations on complaints, including the ability to make declarations as to appropriate monetary damages or other remedies such as injunctions,[15] although constitutional restrictions on the exercise of judicial authority in Australia[16] mean such findings can only be enforced through the federal courts in that country.[17] Despite this technicality, the study catalogued the determinations by the Commissioner during the period selected. In addition, it examined investigative reports by the Commissioner as well as enforceable undertakings given to it.

Although most complaints in Hong Kong are resolved through conciliation,[18] the Commissioner is empowered to issue both investigative reports as well as enforcement notices where necessary. As is the case with the United Kingdom, it will be shown that data privacy rights are principally secured through these measures, rather than through litigation by individuals in courts of law.

At the time this research was compiled, New Zealand remained an outlier as its data privacy authority, the Privacy Commissioner, lacked any formal enforcement powers beyond the ability to investigate complaints and make recommendations.[19] However, since then an updated Act replacing the earlier legislation has come into force that contains compliance powers for the Privacy Commissioner to supplement the existing litigant-reliant remedial mechanisms.[20] For the period studied, therefore, the primary source of enforcement consisted of decisions of the Human Rights Review Tribunal ("the Tribunal") which, instead of courts of law, is the specialist tribunal to which

---

12 The Commissioner's enforcement measures under the European Union's e-commerce rules were only catalogued where the circumstances also constituted a contravention of the Data Protection Act; see European Commission, *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC* [2014] OJ, L 257/73.

13 *Australian Privacy Act 1988*, *supra* note 11, s 40A.

14 *NZ Privacy Act 1993*, *supra* note 11, s 74.

15 *Australian Privacy Act 1988*, *supra* note 11, s 52.

16 *Commonwealth of Australia Constitution Act* 1900, Chapter III.

17 *Australian Privacy Act 1988*, *supra* note 11, s 55A.

18 Privacy Commissioner for Personal Data, *2017-18 Annual Report* (Hong Kong: Office of the Privacy Commissioner for Personal Data, 2018) at 40-42 [*HK PCPD 2017-18 Annual Report*].

19 *NZ Privacy Act 1993*, *supra* note 11, s 23 and Part 8. However, there have been significant investigations of agencies by independent third parties conducted on a voluntary basis; see KPMG & Information Integrity Solutions, *Independent Review of ACC's Privacy and Security of Information* (Wellington: Privacy Commissioner and Accident Compensation Corporation, 22 August 2012).

20 *Privacy Act 2020* (NZ), 2020/31, Part 6 [*NZ Privacy Act 2020*].

complaints concerning contraventions of the data privacy legislation can be referred either by the Commissioner,[21] or by individuals where conciliation fails.

Significant limitations of the methodology employed in the research must be acknowledged from the outset. In the first place, the documented outcomes are taken from information published and accessible on Internet databases. For instance, the United Kingdom only provides data for the most recent two years in relation to some categories of information. As a result, the available data presents only a snapshot in time of the range of regulatory responses. However, as will be seen, this is nonetheless sufficient to reach tentative conclusions as to the relative merits of the different approaches.

III. Litigation by Individuals

In line with the "full functionality" principle referred to above in the Introduction, application of the philosophy underlying Cavoukian's design to the enforcement context militates towards the rights exercised by individuals not being a zero-sum game: choosing to litigate one's rights ought not to foreclose the ability of authorities to investigate the same facts, including the initiation of investigations through their own volition. Applying this in the antipodean context was nonetheless less than straightforward.

Thus, both Australia and New Zealand appear to not provide individuals with the right to litigate contraventions of their data privacy rights in courts of law. Both jurisdictions do, however, provide the means for authoritative adjudication of claims—Commissioner determinations and Tribunal decisions respectively—backed up with enforceable sanctions. It will be seen that significant monetary damages have been awarded in New Zealand and, to a lesser extent, in Australia, together with other non-monetary relief.[22]

In terms of the *GDPR*, therefore, it is likely that both jurisdictions can be said to provide the "right to an effective judicial remedy"[23] and the right to compensation for "material or non-material damage",[24] in addition to more specific remedies such as injunctions.[25] An obvious point of comparison is with litigation in courts of law in other jurisdictions such as the United Kingdom and Hong Kong.

Bygrave discusses the obvious tension between adjudication by specialist adjudicative fora in contrast to normal courts:

> [T]here is also a risk that DPAs construe data privacy legislation in ways that further the cause of data privacy at the expense of other factors that require equal or greater weighting as a matter of *lex lata*. That risk is acute when promotion of data privacy is central to a DPA's formal remit. The judiciary, approaching the

---

21 Technically through the intermediate step of referral to the Proceedings Commissioner.

22 For a discussion on the Australian determinations, see Norman Witzleb, "Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy" in Jason N E Varuhas and N A Moreham, eds. *Remedies for Breach of Privacy* (Great Britain: Hart Publishing, 2018) [Witzleb, "Determinations"]. For a discussion on more recent New Zealand rulings, see *Gunasekara and Singh*, "Upping the Ante", *supra* note 9.

23 *GDPR*, *supra* note 1, art 79(1).

24 *Ibid*, art 82(1).

25 *Ibid*, art 58(2).

> legislation with relatively fresh eyes and formally unencumbered by a pro-privacy mandate, will tend to be better able to resist such bias. Yet, courts' frequent lack of familiarity with legislation, combined with the time pressures of litigation, can result in their failing to appreciate the complexities of the legislation in ways that undermine the correctness of their judgments.[26]

These tensions will be evident in the examples canvassed in this study. As Bennett points out,[27] the public funding needed for the paraphernalia of data protection authorities, unlike courts, requires a political constituency.

The antipodean approach to individual claimants is considered in the first instance.

A. *Australia and New Zealand*

As noted, comparisons between these jurisdictions are apt due to the alternative mechanisms they both provide to individuals to vindicate their data privacy rights through litigation. If New Zealand is first considered, the quasi-judicial nature of its Tribunal aligns proceedings before it closer to those before courts despite the legislative stipulation that "the information privacy principles do not confer on any person any legal right that is enforceable in a court of law."[28]

In the period under scrutiny, the Tribunal considered 47 cases—an average of eight per year. It is important to stress this only included substantive cases, thus excluding interlocutory rulings, strike-out applications and costs applications before the Tribunal. Plaintiffs were successful in 49 percent of these cases.[29]

Of the disputes litigated, 57 percent could be linked to other disputes between the parties, for example involving employment relationships,[30] with the remainder being purely concerned with breaches of data privacy.[31] This contrasts with an earlier study of cases between 2000 and 2010 which found that as many as 80 percent of Tribunal cases were linked to disputes or claims unrelated to data privacy.[32] Despite most cases still concerning collateral matters, the lower proportion in more recent times may evidence greater awareness, on the part of New Zealanders, of their data privacy rights together with the willingness to litigate them independently of the existence of any collateral dispute.

A seminal case was *Holmes v Housing New Zealand Corporation*,[33] which involved the first of New Zealand's information privacy principles which stipulates that personal information may only be collected for a lawful purpose of the agency

---

26 Lee Bygrave, Data Privacy Law: An International Perspective (United Kingdom: Oxford University Press, 2014) at 4.

27 CJ Bennett, The Privacy Advocates: Resisting the Spread of Surveillance (Cambridge, Massachusetts: MIT Press, 2008) at 199.

28 *NZ Privacy Act 1993*, *supra* note 11, s 11(2).

29 Success was where the plaintiff obtained a remedy amounting to either monetary compensation or a specific remedy such as an injunction or declaration.

30 *Hammond v Credit Union Baywide* [2015] NZHRRT 6 [*Hammond*].

31 A good example, discussed below, is *Armfield v Naughton* [2014] NZHRRT 48.

32 Gehan Gunasekara and Alida Van Klink, "Out of The Blue? Is Litigation Under The Privacy Act 1993 Addressed Only at Privacy Grievances?" [2011] 17 Canta LR 229.

33 [2014] NZHRRT 54 [*Holmes*].

and be necessary for that purpose.[34] The plaintiff was a beneficiary who chose to forgo a benefit (*ie*, income-related rent) rather than disclose information requested by a state agency which was seeking to collect information strictly unnecessary for its own purposes, but which was pursuant to an inter-agency agreement with another state agency. The Tribunal opined:

> Principle 1 is the overarching privacy principle from which the others flow and further given the need to promote and protect individual privacy, the term "collect" must be given a broad and purposive interpretation. It includes the elements of "gathering together", seeking or acquiring not just receiving.[35]

The Tribunal further stated that the OECD Privacy Guidelines:

> [R]ecognise that collection is not an event (ie receipt of the data) but a process for the collection of data. That process must be in place, prior to the receipt of the data and contain the safeguards of "lawful and fair means" and "knowledge or consent".[36]

Crucially therefore, it was found that Principle 1 applied prior to the actual receipt of personal information, including the instance (as had occurred on the facts of *Holmes*) where no personal information had actually been collected by the agency involved.[37]

In the case of *Taylor v Orcon*,[38] the Tribunal signalled a significant reorientation in its attitude to causation:

> It is not necessary for the cause to be the sole cause, main cause, direct cause, indirect cause or "but for" cause. No form of words will ultimately provide an automatic answer to what is essentially a broad judgment.[39]

The move away from a strict view of causation is justified due to the evolving nature of informational technologies, such as algorithmic decision-making and artificial intelligence, where it may be impossible to identify the role played by one data point amongst many.

Despite there being few Tribunal decisions that have been successfully reversed on appeal to the High Court, an exception arose in *Attorney-General v Dotcom*.[40] In this instance, the Court found that the complainant's request to access his data was vexatious and, further, that the injury alleged to have been suffered was connected more with the underlying extradition proceedings that the request concerned and the perceived treatment he had received from the authorities than the withholding of his information request.[41]

---

34 *NZ Privacy Act 1993*, *supra* note 11, Principle 1.
35 *Holmes*, *supra* note 33 at para 71.
36 *Ibid* at para 75.
37 *Ibid* at para 76.
38 [2015] NZHRRT 15.
39 *Ibid* at para 61.
40 [2018] NZHC 2564.
41 *Ibid* at paras 188, 222-223; at the time of writing, the decision has been partly reversed by the Court of Appeal in *Dotcom v Attorney-General* [2020] NZCA 551 (CA).

There were far fewer Australian determinations than Tribunal decisions in New Zealand: only 27 in the period under study, or less than five per year. On the other hand, plaintiffs were successful in 93 percent of the determinations. However, it was evident from the facts that 41 percent were in some way linked to disputes between the parties unrelated to privacy.

Witzleb has undertaken a detailed scrutiny of the determinations, noting monetary awards "remain relatively conservative, with amounts ranging between $1,500 and $20,000."[42] He notes that awards for non-economic loss have yet to follow the approach taken in sex discrimination and sexual harassment cases and reflect "current community expectations and standards."[43] In this aspect Australia appears to lag behind New Zealand where it has been observed that there has been a convergence between damages awarded under human rights and privacy legislation, possibly facilitated by the Tribunal being the specialist adjudicator in both areas.[44]

Where economic losses such as loss of income and benefits are concerned, however, Witzleb notes that difficulties tend to exist in establishing their "causal link to the privacy interference."[45] Although this has also been the case in New Zealand, it has been seen that the Tribunal's approach has been to compensate for the impediment through more generous awards for non-economic losses, such as injury to feelings and humiliation. Although these are also available in Australia,[46] it is evident that awards have been significantly smaller there than in New Zealand.

Tables 1 and 2 depict the overall comparisons, as to total damages awards, between the Tribunal decisions and determinations. *Hammond* was excluded on the basis that it is somewhat of an outlier whose inclusion would skew the data.[47] It is immediately evident that there is a significant discrepancy in the median as well as range of awards which cannot be explained by the fairly minimal differences in exchange rates between the two countries.

Despite these differences, there is much common ground between the approaches of the Tribunal and Commissioner. Although few determinations have been appealed to the Administrative Appeals Tribunal or Federal Court in Australia, the few such instances have resulted in useful guidance as to the principles that must be applied by the Commissioner when making determinations. For example, in *Rummery v*

Table 1

Damages (NZ) (2013-2018) (Excluding *Hammond*):	
Range	NZD400 - NZD90,000
Mean	NZD17256
Median	NZD13187

42 Witzleb, "Determinations", *supra* note 22 at 407.
43 *Ibid*.
44 *Gunasekara and Singh*, "Upping the Ante", *supra* note 9 at 467.
45 Witzleb, "Determinations", *supra* note 22 at 407.
46 *Australian Privacy Act 1988*, *supra* note 11 at ss 52(1AB)(a)-52(1AB)(b).
47 *Hammond*, *supra* note 30, involves the largest award thus far of NZD168,000.

Table 2

Damages (Aus) (2013-2018):	
Range	AUD1,000 - AUD20,000
Mean	AUD8095
Median	AUD7500

Federal Privacy Commissioner, it was stated that guidance should be taken from case law interpreting sex discrimination legislation;[48] redress should follow harm; awards should be "restrained but not minimal; aggravated damages being available in "appropriate" cases; and the individual circumstances of the complainant should guide awards, rather than the more objective "reasonable person" test—in other words, the eggshell skull principle should apply.[49]

Likewise in *EQ and Office of the Australian Information Commissioner (Freedom of information)*,[50] it was stressed that although the principles of tort law are useful as a guide, the courts must ultimately defer to the words of the statute. These statements point to data privacy law being *sui generis* and not merely an appendage of existing common law remedies. The *EQ* determination also raised issues of causation as the facts concerned an employee who was the subject of investigation for an alleged offence whose identity had been confirmed to news media by his employer. The publicity accompanying the incident, together with the complainant's own role in the alleged offence, complicated the difficulty of linking the harm suffered by him to the employer's conduct.[51] Although economic loss could not therefore be established, $8000 was awarded for non-economic loss.[52]

In statements resonating with those made by the Tribunal in *Taylor v Orcon* in New Zealand, the Administrative Appeals Tribunal stated that "a 'but for' analysis is not a sufficient test [for] causation, although it may be a guide" and "where there are multiple elements, each one sufficient on its own to have caused the loss, the causation test may be considered satisfied by each one of them".[53]

In *'KA' and Commonwealth Bank of Australia Ltd*,[54] the Commissioner refused to award damages for economic loss, especially as these pertained to related employment proceedings between the complainant and a third party and the claim that the

48 *Hall v A & A Shiban Pty Ltd* (1989) 20 FCR 217 at 282, per French J.

49 [2004] AATA 1221 at para 32.

50 [2016] AATA 785 at para 39 [*EQ*].

51 *Ibid*. See also *EQ and Great Barrier Reef Marine Park Authority* [2015] AICmr 11 (2 February 2015) at paras 80-81, where the Commissioner stated: "The complainant could not have suffered. . . loss but for his own conduct. . . [he] accepts that he took a marine conservation research boat into the marine park and fished unlawfully in a marine conservation zone. . . it is appropriate to award damages to recognize the humiliation the complainant suffered, while still recognizing that the complainant was the primary contributor to his own non-economic loss.

52 *EQ*, *supra* note 50 at para 61, where the Commissioner's award of $5000 was increased by the Administrative Appeals Tribunal on the basis that the complainant had "paid the fine rather than opting to defend himself upon the basis of honest and mistaken belief due to the alleged inaccuracies in his navigation system" and had been "assured that the matter of his fine would not be made public".

53 *Ibid* at para 47.

54 [2015] AICmr 86.

amount she had obtained in settling it would have been greater but for the data privacy contravention: "I do not think it can be said that if the principal had not accessed the complainant's [single-view]. . . profile, the complainant would now be in a position of having received from him an additional $100,000."[55]

The reluctance to award compensation in what were essentially disputes over matters unrelated to data privacy is a theme in both jurisdictions as clearly, privacy forums were cautious not to allow recovery through data privacy remedies for grievances over matters other than privacy. As has been seen in both Australia and New Zealand, the specialist privacy adjudicators have shown the willingness to find that an interference with privacy has occurred where it was a contributing cause, even if not the main or "but for" cause. Where remedies are concerned, however, Witzleb has suggested that "the assessment of compensation should reflect the contribution of other causes for which the respondent does not bear responsibility."[56] Such a nuanced approached has yet to be adopted in either jurisdiction.

Although specialist privacy adjudicators have led through providing means for individuals to litigate their data privacy rights, it will be seen that the right to an effective judicial remedy and to compensation for material or non-material damage is less attainable in the other jurisdictions examined in this study that provide recourse to their citizens through courts of law. These are examined next.

B. *United Kingdom*

Litigation pursued under data protection legislation[57] was sparse, with only six substantive cases in the period of the survey.[58] In most of these cases, plaintiffs also invoked either the tort of misuse of private information or the tort of defamation.[59] The majority (*ie*, four) of these cases were against public sector defendants;[60] the remainder (*ie*, two) were against private sector defendants.[61] It was evident that in all but one of the cases that the parties had been engaged in a collateral dispute which led to the alleged privacy infringement.[62]

Plaintiffs were successful in four of the six cases—a 67 percent success rate. However, successful plaintiffs only secured nominal or modest damages.[63] Difficulties in establishing causation may account, at least in part, for this. For instance, it was

---

55 *Ibid* at para 81.

56 Witzleb, "Determinations", *supra* note 22 at 393.

57 For the period studied this was under the *UK Data Protection Act 1998*.

58 One of these, *Trushin v National Crime Agency* [2014] EWHC 3551 (Admin), was technically an interlocutory decision where the court refused to strike out the claim or give summary judgment; the recent case of *Wm Morrison Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339 was not included as it only engaged the data protection legislation indirectly through breach of statutory duty and sought to establish vicarious liability on the part of an employer for breaches committed by a malicious employee.

59 *Vidal-Hall v Google Inc* [2015] 3 WLR 409 (CA) [*Vidal-Hall*]; this study is not concerned with outcomes under these causes of action.

60 *Lyons v Chief Constable of Strathclyde* [2013] CSIH 46.

61 *Halliday v Creation Consumer Finance Limited* [2013] EWCA Civ 333 [*Halliday*].

62 The exception being *Vidal-Hall, supra* note 59.

63 For example, GBP 750 in damages for distress and GBP 1 for nominal damages in *Halliday*, *supra* note 61.

stated in *Halliday v Creation Consumer Finance Limited* that "[t]he breach was, as I see it, of a limited nature. It did not lead to loss of creditor reputation. There may well be other cases where there is a loss of some housing benefit or opportunity or credit facilities and so on. That was not this sort of case."[64]

The United Kingdom courts also exhibited mixed signals as to their appreciation of the human rights underpinnings of data privacy. For example, it was stated that:

> [T]he field of discrimination is... not a helpful guide for the purposes of data protection. Discrimination is generally accomplished by loss of equality of opportunity with far reaching effects and is liable to cause distinct and well-known distress to the complainant.[65]

On the other hand, in a case somewhat along the lines of *Taylor v Orcon* in New Zealand, a technical failure to comply with consumer credit legislation had rendered a debt unenforceable; however, the erroneous reporting of default had potentially far more serious consequences for the individual concerned and was accordingly recognized by the Court.[66]

Despite the paucity in court litigation, a decision in the period with wider ramifications was *Vidal-Hall v Google Inc*,[67] where it was held to be arguable that browser-generated information was personal data, and that the tracking and collating of information relating to individuals' internet usage and subsequent disclosure of the same through targeted advertising to third parties without the individuals' consent or knowledge contravened data privacy norms. Furthermore, it was held that damages for distress alone were sufficient without the need to show accompanying pecuniary loss.[68]

This marked a significant turning point in the United Kingdom. Previously, Jay noted a reluctance by courts to award damages for hurt feelings alone as "[t]he courts expect individuals to face life with a degree of stoicism. They are not sympathetic to the idea that any unhappy experience should result in a financial windfall."[69]

The deficiency has now, in any event, been addressed by the United Kingdom's Data Protection Act 2018.[70]

C. *Hong Kong*

In a commentary on the effectiveness of data privacy enforcement in Hong Kong, Alana Maurushat gives four reasons why the territory's data protection legislation's provision of a judicial remedy for individuals, including the ability to claim damages

---

64 *Ibid* at 7.

65 *Ibid* at 6.

66 *Grace & Anr v Black Horse Ltd* [2014] EWCA Civ 1413 at 9, per Briggs LJ.

67 *Vidal-Hall*, *supra* note 59.

68 Under the *UK Data Protection Act 2018*, *supra* note 8, s 13, it was not previously possible to obtain damages for distress alone.

69 Rosemary Jay, *Data Protection Law and Practice*, 4th ed (United Kingdom: Sweet & Maxwell, 2012) at 509 [Jay, *Data Protection*].

70 *UK Data Protection Act 2018*, *supra* note 8, ss 168-169.

for "injury to feelings",[71] has been largely symbolic:

> First, no one has ever succeeded in court. Second, Hong Kong courts generally do not invite class actions. Third, the onus is on the plaintiff to show that there was a failure on the part of the data user to take all reasonably practicable steps to secure the data. . . Last, the Privacy Commissioner does not have the power to assist citizens in litigation, in which case affected individuals have to hire their own legal counsel.[72]

The evidence supports these conclusions. Only a handful of court proceedings invoking the Ordinance have been undertaken and these are listed on the website of Hong Kong's data protection authority.[73] In the period studied for this research, only two cases were pursued; one of them was an interlocutory matter concerning delay in correcting an inaccurate credit status,[74] the other involved litigation over a matter unrelated to privacy, in which the Ordinance was unsuccessfully invoked to prevent discovery sought in the litigation.[75]

A focus on individual litigation, however, only reveals a very small part of the picture as to the enforcement of data privacy rights in Hong Kong. Maurushat notes the main strategy of the Commissioner is on education and mediation between data subjects and data controllers.[76] For example in the 2017-2018 reporting period, despite a total of 1619 complaints being received,[77] 850 of these were dealt with through non-binding "recommendations",[78] with 273 compliance checks undertaken.[79] In only 41 instances flowing from the complaints and compliance checks were the parties in breach required to take remedial action of some kind through the issuance of warnings or enforcement notices.[80] A tiny number, 16, were referred to the police with the consent of the complainants involved.[81] These further types of enforcement are discussed below.

IV. Regulator-led Enforcement

It has been seen that the availability of judicial remedies across the jurisdictions surveyed is variable. Even where interferences with privacy have occurred, difficulties

---

71 *HK Personal Data Ordinance 1995*, *supra* note 11, s 66.

72 Alana Maurushat, "Who Let the Cat out of the Bag? Internet Data Leakage and Its Implications for Privacy Law and Policy in Hong Kong" (2006) 36(1) HKLJ 7 [Maurushat, "Internet Data Leakage"].

73 Privacy Commissioner for Personal Data, online: <https://www.pcpd.org.hk/>.

74 *Lee Kwok Tung Albert v Chiyu Banking Corp. Ltd* [2018] HKCA 123.

75 *Chan Yim Wah Wallace v New World First Ferry Services Ltd* HCPI No. 820 of 2013.

76 Maurushat, "Internet Data Leakage", *supra* note 72 at 4.

77 Eighty percent of complaints were against private sector organisations while 20 percent were against public sector organisations, including government departments; see *HK PCPD 2017-18 Annual Report*, *supra* note 18 at 30.

78 *Ibid* at 51.

79 *Ibid*. Although data breach notification is not the focus of the present research, it is instructive that 116 of such notifications occurred, resulting in compliance checks in all of them: see *ibid* at 34.

80 *Ibid* at 50. No further statistics are available, however, as to the number or subject of these or their ultimate outcome.

81 *Ibid* at 49.

exist with establishing economic loss—especially when the context of litigation is linked to claims other than privacy—whilst assessment of non-economic loss has been equally problematic. One suggested solution is to see any loss of privacy as per se harms for which damages are available.[82] Under this approach damages are seen as "necessary for the vindication of the right in question."[83]

Although attractive, such an approach has its own drawbacks. For instance, if damages are to be more than nominal, it may insufficiently differentiate between types of harm especially when it is likely to affect individuals other than the plaintiff. Witzleb puts the issue in a nutshell:

> Breaches of human rights statutes can also cause remedial difficulties when a strong response is called for, yet actual losses suffered are small and the statute does not allow the award of exemplary damages. In these cases, recourse to the purpose of vindication has been made to justify the award of a substantial amount of damages.[84]

However, a more effective regulatory scheme ought to provide means of enforcement other than through individual litigants, as is indeed stipulated under the requirements of the *GDPR*.[85] In particular, the regulator must be able to respond to the breach in a manner that does not require a conceptual link to an individual litigant with the attendant difficulties of establishing causation and damage. Furthermore and importantly, a focus on one or even a small number of individuals can lead to the overlooking of serious underlying deficiencies in organizational practices that may well be the root cause of the failure. The remainder of this article accordingly examines the experience of three jurisdictions where enforcement is led by regulators.

A. *Investigative Reports*

A useful source of information regarding data privacy practice—compliance and performance[86]—are the authoritative reports compiled by data privacy authorities in the jurisdictions where they have an enforcement role. These often follow enforcement notices in Hong Kong,[87] and are often linked to enforceable undertakings in Australia. The broadly comparable jurisdictions therefore are Hong Kong and Australia, where Commissioner-initiated investigation reports were also available. The most comparable reports in the United Kingdom are monetary penalty notices.

In the time frame of this study, there were 14 investigative reports published in Hong Kong under a legislative provision conferring discretion on the Commissioner

---

82 Nicole Moreham, "Compensating for Loss of Dignity and Autonomy" in Jason N E Varuhas and N A Moreham, eds. *Remedies for Breach of Privacy* (Great Britain: Hart Publishing, 2018).

83 Witzleb, "Determinations", *supra* note 22 at 393.

84 *Ibid* at 394.

85 Articles 57 & 58 confer powers on supervisory authorities—especially art 57(2), which confers a power to order corrective measures—whilst Chapter VIII contains articles 83 & 84 relating to administrative fines and penalties.

86 See Malcolm Crompton and Michael Trovoto, *The New Governance of Data and Privacy: Moving beyond compliance to performance* (Sydney: Australian Institute of Company Directors, 2018).

87 The details of all enforcement notices are not made separately available.

to publicise the results of investigations as well as any recommendations arising from them of wider relevance where they concern other data controllers who may be affected by similar issues to the controllers under investigation.[88] While not, therefore, a comprehensive catalogue of the outcome of all investigations carried out by the Commissioner, the reports nonetheless reveal a range of concerns and useful conclusions to be drawn from them of wider relevance to data privacy governance globally.

Scrutiny of the reports reveal that two thirds of the investigations were Commissioner-initiated, although often at the prompting of news media,[89] while a third resulted from complaints, usually by multiple complainants.[90] Some were the result of "sweeps" undertaken on the Commissioner's own initiative.[91]

A report of considerable significance for the interpretation of data privacy principles globally was that concerning *Glorious Destiny*.[92] This involved those supplying the "Do No Evil" App which allowed smart phone users to access information on individuals linking their bankruptcy, litigation, criminal offending and company data. The information was sourced from public registers or from publicly available sources, although not all of the latter were readily accessible.

The comprehensive 30-page report usefully undertakes a detailed examination of the purposes for which the various public registers and other public data sources from which the App sourced its information existed.[93] It also traverses the distinct issues raised by the App, including: rearrangement of personal data collected from the public domain; data subjects being ignorant as to who is accessing their data; loss of control over further use of the data; the data made accessible by the App not being accurate, up-to-date, or sufficiently comprehensive and jeopardizing an offender's chances of rehabilitation.[94]

Two data protection principles were relevant to the investigation. Principle 1(2), which requires that personal data are collected by means that are both "lawful" and "fair", was found not to have been contravened as the sources were public ones.[95] However, Principle 3(1), which requires that personal data cannot be used for a new purpose without the prescribed consent of the data subject, was found to have been contravened.[96]

---

88 *HK Personal Data Ordinance 1995*, *supra* note 11, s 48(2).

89 For example, the Commissioner was alerted by the media to a leak of the Hong Kong Police Force's internal documents through a website; see R13 - 15218, *Investigation Report: The Hong Kong Police Force leaked internal documents containing personal data via Foxy* (24 October 2013).

90 For example, see the *Glorious Destiny Report*, *infra* note 92.

91 For example, one concerning blind recruitment advertisements that failed to identify either the employer or recruitment agency so as to solicit personal information; see R14 - 6242, *Investigation Report: unfair collection of personal data by the use of "blind" recruitment advertisement* (29 May 2014).

92 R13 - 9744, *Glorious Destiny Investments Limited and Brilliant United Investments Limited Publicly Disclosed Litigation and Bankruptcy Information Collected from the Public Domain to Their Customers via Smartphone Application "Do No Evil"* (13 August 2013) [*Glorious Destiny Report*].

93 For example, court lists were to facilitate open justice by notifying members of the public as to matters before the courts at the time (lists being removed afterwards) and to enable parties, witnesses and related persons to attend at the scheduled times.

94 For instance, in relation to bankruptcy which has clear time-limits on accessibility, whereas the App made the information available indefinitely; *Glorious Destiny Report*, *supra* note 92 at para 49.

95 *HK Personal Data Ordinance 1995*, *supra* note 11, Schedule 1.

96 *Glorious Destiny Report*, *supra* note 92. The actual wording was slightly different at the time of the Report but is the same in substance.

Glorious Destiny is important in terms of legislative design. The architecture of the Hong Kong data protection principles meant that whilst collection of the information was not a contravention, its subsequent use was. By contrast, New Zealand's Information Privacy Principles 10 and 11 provide that where an agency believes on reasonable grounds "that the source of the information is a publicly available publication and that, *in the circumstances of the case, it would not be unfair or unreasonable to use [or disclose] the information*", it may use or disclose it.[97] It is arguable that the sourcing of personal data is better placed in the collection principles and those concerned with the fairness of collection[98] rather than grafted on as an exception to processing. It is certainly possible that the emphasized qualification contained in the New Zealand wording may enable a similar result to be reached as in *Glorious Destiny*, but this remains to be seen. At the very least, the Hong Kong report will serve as compelling authority on the point.

In Australia, there are eleven Commissioner-initiated investigations in the period studied. As is the case with the United Kingdom's monetary penalties and other enforcement activities, the practice is to publicise all such investigations. All the Australian Reports involved contraventions of data security and all also involved disclosure of personal information but stemming from the security breach.[99] Some were the result of mistaken uploads to publicly accessible websites.[100]

One investigation also concerned both data quality (accuracy) and indefinite retention (beyond purpose). This was the Joint Investigation of Ashley Madison which was undertaken by both the Privacy Commissioner of Canada and by the Australian Information Commissioner.[101] This followed the 2015 hack of the adult dating website, potential compromise of personal information of approximately 36 million users and subsequent disclosure of information by the hackers. Both the scale and sensitivity of the information were invoked by the authorities concerned in undertaking the investigation.[102]

Crucially, the investigation delved into the factors that caused or led to the data breach. Clearly, given the sensitivity of the information and foreseeable potential impact on individuals should it be compromised, the company was found not to

---

97 *NZ Privacy Act 1993*, *supra* note 11, Principles 10(1)(a) and 11 (b) respectively [emphasis added]; these Principles remain unchanged in the *NZ Privacy Act 2020, supra* note 20.

98 *NZ Privacy Act 1993, ibid*, Principles 1-4.

99 See Office of the Australian Information Commissioner, *Multicard Pty Ltd: Own motion investigation report* (Canberra: Office of the Australian Information Commissioner, 1 May 2014), which was initiated by the Commissioner after receiving information that personal information collected by Multicard had been made publicly accessible online. The information included names, dates of birth, addresses, ID numbers, partial credit card numbers, reference numbers and photographs. The information was downloaded by at least one third party.

100 Office of the Australian Information Commissioner, *Department of Immigration and Border Protection: Own motion investigation report* (Canberra: Office of the Australian Information Commissioner, 1 November 2014), where personal information of approximately 10,000 asylum seekers was available on a Government website for 8 days as a result of a mistaken upload.

101 Office of the Privacy Commissioner of Canada, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner* (Ottawa: Office of the Privacy Commissioner of Canada, 1 August 2016) [*Ashley Madison Investigation*].

102 *Ibid* at para 3. The Privacy Commissioner of Canada's involvement was on account of the Ashley Madison website being headquartered in Canada.

have taken reasonable security measures.[103] However, another contributing factor was a failure to verify the email addresses given by users,[104] often email addresses belonging to a third party such as a work email, compounding the harm that resulted from the breach.[105]

Perhaps the most significant cause, however, was retention of personal information beyond reasonable time frames. In a case of actual application of the lyrics of the famous song, "you can check out anytime you like but you can never leave",[106] practices such as the indefinite retention of deactivated accounts,[107] retention of information from inactive profiles, retention of information following a "full delete", including charging a fee for complete deletion, were found not to be justified.[108] These clearly created risks for past and present users, and the recommendations made to address them—including retention policy review and retention schedule implementation—are instructive in the context of data privacy governance more generally.[109]

The *Ashley Madison* investigation is not, however, an isolated incident as almost half (*ie*, five) of the Australian investigations revealed a failure to destroy or de-identify personal information that was no longer needed.[110] This is a theme that exists across all three jurisdictions.

The outcome of the investigations in Australia ranged from where the agencies investigated undertook remedial actions,[111] the requirement for independent audits and, more recently, enforceable undertakings by the agencies subject to the investigation. Jay notes that enforceable undertakings are the "regulatory weapon of choice" for enforcing data privacy requirements.[112] She further notes that whilst their precise legal status is somewhat ambiguous—the traditional view being they are enforceable as contracts—in reality they serve as a "formal public warning".[113] In this regard, they have some similarity with the publicly notified settlements of the Federal Trade Commission in the United States.[114]

Prosecutions were another regulatory tool in both Hong Kong and the United Kingdom. In the former, the prosecutions are referred to the police and not conducted

---

[103] In addition to specific weaknesses such as poor key and password management, it did not have an adequate and coherent information security governance framework; see *ibid* at paras 76-81.

[104] *Ibid* at paras 146-149. These were held to constitute personal information.

[105] One recommendation was to allow users, in future, to join the website without providing an email address; see *ibid* at para 168.

[106] The Eagles, "Hotel California" (1977).

[107] On the justification users might return, see *Ashley Madison Report*, *supra* note 101 at para 112.

[108] *Ibid* at paras 111-121. One justification advanced (but rejected) was that the retention of information was in case of disputed credit card payments; statistics presented established that the majority of such queries occurred within 3 months and 98 percent within 6 months; see *ibid* at para 110.

[109] *Ibid* at para 133.

[110] See, for example, Office of the Australian Information Commissioner, *AAPT and Melbourne IT: Own motion investigation report* (Canberra: Office of the Australian Information Commissioner, 31 August 2016), where compromised servers contained some old customer information that AAPT had failed to destroy or de-identify after it was no longer in use.

[111] Which were often reviewed by the Commissioner with further recommendations where necessary.

[112] Jay, *Data Protection*, *supra* note 69 at para 20-90.

[113] *Ibid* at para 20-92.

[114] See Daniel Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy" (2014) 114 Colum L Rev 583; Gehan Gunasekara and Jingyi Xiong, "Lost in Translation? Privacy and Unfair or Deceptive Acts or Practices in Commerce in the United States" (2016) 22 NZBLQ 162.

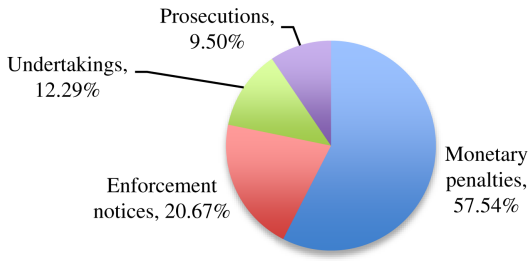
by the Commissioner (as is the case in the United Kingdom). Maurushat notes that there has been a paucity of cases referred for prosecution in Hong Kong.[115] As several privacy breaches involved failures by the police themselves, she further notes the weakness of such a structure for conducting prosecutions.[116]

Jay's assertion aside, the largest category of enforcement in the United Kingdom, as well as that with the greatest impact, are monetary penalty notices which therefore merit separate consideration.

B. *Monetary Penalty Notices*

On its website the United Kingdom Information Commissioner's Office usefully provides information as to the enforcement actions undertaken in all categories over the most recent two-year period. For the time frame of the present study, this data is shown in Graph 1 below. Whilst undertakings, prosecutions and enforcement notices all featured, it is evident the single largest category consisted of monetary penalty notices.

Graph 1. Enforcement Actions (Two years, 2017-2018)[117]



168 of such notices were issued in the period studied. The vast majority were in respect of direct marketing and unsolicited emails. The next largest category, however, concerns security lapses, which amounted to 29 percent while wrongful disclosure of personal information accounted for 14 percent of notices. The penalties imposed ranged from GBP 250 to GBP 500,000. Most involved large-scale privacy lapses or those of a sensitive nature such as health or financial information.[118]

A recurrent theme in security breaches was a failure to adequately dispose of information no longer needed, including a failure to follow-up with actual disposal

---

115 Maurushat, "Internet Data Leakage", *supra* note 72 at 4.

116 *Ibid*.

117 Information Commissioner's Office, United Kingdom, online: <https://ico.org.uk/action-weve-taken/enforcement/>.

118 Information Commissioner's Office, *Bayswater Medical Centre* ENF0722653 (London, United Kingdom: Information Commissioner's Office, 21 May 2018), where highly sensitive medical information was left in an empty building by a general practice after it moved for more than 18 months; and see Information Commissioner's Office, *British Pregnancy Advice Service* ENF0439709 (London, United Kingdom: Information Commissioner's Office, 28 February 2014).

or destruction. This included insecure disposal of hard drives containing personal data,[119] filing cabinets being sold at auctions,[120] or leaving behind equipment containing data whilst vacating premises.[121] Mistaken uploads to the Internet also featured.[122]

Two monetary penalty cases during the period studied merit specific discussion. The first, *Equifax Ltd*,[123] involved the large-scale hack of the company's United States parent which also compromised the data of up to 15 million United Kingdom residents. Equifax, a major credit reference agency, provided an identity verifier service that was originally hosted in the United States but subsequently migrated to the United Kingdom in 2016.[124] However, personal information pertaining to the service was retained in the United States, leading to the finding that "the process for migrating this data to the UK, and its subsequent deletion in the US, was insufficient and/or not adequately effective."[125]

The purposes for retaining the information, which included plaintext passwords, had not been sufficiently articulated.[126] The stated purpose, fraud prevention, was found not to be necessary given the company's own cryptography standards and other fraud prevention techniques in use at the time.[127] There was also a failure to carry out appropriate audits of the parent company as permitted through its contractual arrangements.[128] In deciding to impose a GBP 500,000 penalty, the highest amount then available, the Commissioner referred to:

> [T]he multiple, systemic and serious inadequacies identified. . . in respect of the way in which Equifax Inc processed data on behalf of Equifax Ltd and Equifax Ltd's failure to adequately address these shortcomings. . . The Commissioner has also considered the importance of deterring future contraventions of this kind, both by Equifax Ltd and by others.[129]

The second case involving Facebook stemmed from the Commissioner's ongoing investigation into the use of data analytics for political purposes.[130] The investigation arose due to what may be described as a "Trojan Horse" App (the "App") used by around 300,000 Facebook users worldwide. However, as the App was able to also

---

[119] Information Commissioner's Office, *NHS Surrey* ENF0452677 (London, United Kingdom: Information Commissioner's Office, 18 June 2013).

[120] Information Commissioner's Office, *Department of Justice Northern Ireland* ENF0450748 (London, United Kingdom: Information Commissioner's Office, 14 January 2014).

[121] Information Commissioner's Office, *Chief Constable of Kent Police* ENF0476958 (London, United Kingdom: Information Commissioner's Office, 17 March 2014).

[122] Information Commissioner's Office, *Aberdeen City Council* ENF0437877 (London, United Kingdom: Information Commissioner's Office, 29 August 2013).

[123] Information Commissioner's Office, *Equifax Ltd* RFA0699842 (London, United Kingdom: Information Commissioner's Office, 19 September 2018).

[124] *Ibid* at para 20.

[125] *Ibid* at para 21.

[126] *Ibid* at para 34.

[127] *Ibid* at para 25.

[128] *Ibid* at para 35.

[129] *Ibid* at para 45.

[130] Information Commissioner's Office, *Facebook Ireland Ltd & Facebook Inc* (London: Information Commissioner's Office, 24 October 2018) at paras 22-24.

collect information about their friends, as many as 87 million individual's data may have been collected; of these, around 1 million were Facebook users in the United Kingdom.[131]

The information harvested by the App included users' profiles, their likes, the pages liked by their friends, friend lists and Facebook messages.[132] Somewhat more concerning was evidence that the data collected included not only the identity of message recipients but also included the content of the messages.[133] Unsurprisingly, breaches as to the principle of fairness of collection as well as of adequate data security were found.[134]

The circumstances in which Facebook had allowed the breaches to occur, however, is more instructive. The App in question was subject to review in May 2014, following which further permissions to access the Facebook platform was denied.[135] Despite this, a grace period allowed continued access until May 2015. Critically, however, even when access ended after this:

> [The] application developers... were able to retain detailed information about users of their apps and their friends that they had previously collected via their apps. *The Facebook Companies did not at that point require them to delete such data, or any of it.*[136]

The emphasized words support the rationale behind the *GDPR*'s Right to Erasure or "Right to be Forgotten", especially its requirement that when data is to be erased, reasonable measure are needed to inform downstream users to whom the data has been previously transmitted.[137]

V. Conclusion

This article has considered a snapshot of four jurisdictions from the standpoint of how they enforce data privacy rights. Against the Cavoukian privacy by design benchmarks, it has been first shown that there is a close parallel between regulators being proactive and transparency, particularly as regards their educative function. The investigative reports of regulators also contain important lessons—for instance, in how information gathered from public registers may be used—that are of wider relevance outside their own jurisdiction. The reports are also of relevance to law reformers especially when designing the architecture of future privacy principles.

Furthermore, the research has demonstrated that in terms of full functionality, providing individuals with rights to litigate their data privacy rights tend to be ineffective except where specialist adjudicative fora exist. Such litigation also tends to be associated with collateral disputes in which the complainants are involved and

---

131 *Ibid* at para 37.
132 *Ibid* at para 28.
133 *Ibid*.
134 *Ibid* at para 9.
135 *Ibid* at para 35.
136 *Ibid* [emphasis added].
137 *GDPR, supra* note 1, art 17(2).

consequently arose over matters of which they were aware such as where personal data was being collected from them or where they had requested access to personal data.

By comparison, regulator-led measures tend to focus on large-scale security lapses and harvesting of personal data, of which individuals concerned are often unaware. These problems tend also to have the potential to affect larger numbers of individuals and regulator-led measures thus often address the root cause of the failures, such as the retention of data when it was no longer necessary. This enables regulators to act proactively to prevent future incidents. Finally, these systemic measures also serve to highlight the need for normative rules, such as a right to erasure or a right to be forgotten.