FROM WALKING THE TIGHTROPE TO A WALK ON THE BRIDGE: THE LESSONS FROM THE UNITED STATES SUPREME COURT DECISION IN *SPOKEO INC v ROBINS*

Inura Fernando*

Abstract

This paper will discuss lessons for New Zealand data privacy law from the United States Supreme Court decision in Spokeo Inc v Robins*. This paper will explore the policy context surrounding data aggregators. It will present the case for a regulatory approach and question the effectiveness of the status quo in addressing harms posed by data aggregators. This paper champions a regulatory model based on sui generis legislation to address the prospective privacy harms stemming from data aggregators such as Spokeo.*

> Privacy, and the associated control of personal data and how it is used, is vital to a sense of personal autonomy. The feeling of being watched and controlled is antithetical to people having the freedom to make their own choices and live their lives how they wish.
>
> New Zealand Council for Civil Liberties[1]

I. Introduction

Technology is not neutral; it takes on the values of its creators. Human rights issues in the modern-day are not confined to cases of torture or voter suppression. Modern human rights violators, whether as individuals or as organisations, have

* BHSc/LLB (UOA), LLM (Second Class Hons, First Division) in Human Rights Law, University of Auckland. Enrolled Barrister and Solicitor of the High Court of New Zealand. I would like to acknowledge the unerring love and support of my parents, Mala and Lal Fernando. I want to especially thank Associate Professor Gehan Gunasekera for his kind support and guidance. I want to acknowledge the advice and kind support of Associate Professor Stephen Penk, I want to thank Dr Bill Hodge for his support and advice, and I want to acknowledge the efforts of the staff of the Privacy Commissioner for responding to my queries and information requests.

1 New Zealand Council for Civil Liberties "Submission to the Justice and Electoral Committee on the Privacy Bill".

become adept to the changes of the information age, which means data aggregation can be a tool in their modus operandi. From white supremacists planning savage, racist attacks, to government bureaucrats intent on violating the civil rights of citizens or immigrants, bad actors now have the manipulation of data and datasets to aid them. Even if such entities are not themselves data aggregators, bad actors can utilise their services for nefarious purposes. Therefore, the regulation of data aggregators is a putative human rights issue.

This article has the following key aims. It hopes to encourage the New Zealand legal community, policy makers and the New Zealand public to join calls to regulate data aggregators in light of the harms they pose in respect of data privacy law. It calls into question the effectiveness of the status quo, represented by Privacy Act 2020, Credit Reporting Privacy Code 2004, Human Rights Review Tribunal (HRRT) cases and the jurisprudence of the New Zealand Courts. This article will draw on lessons from the United States Supreme Court case, *Spokeo Inc v Robins*, and attempt to relate it to New Zealand law. It attempts to provide an understanding of the contextual issues that need to be first understood before further analysis can be discussed. These issues relate to overall questions about what is so unique about data aggregators that warrant separate, targeted regulation. It will also acknowledge some of the limitations of the analysis. It will present some key arguments that call for a regulatory approach towards data aggregators. Finally, it will attempt to present some foundations of a proposed model to regulate data aggregators, separate from the status quo.

It is important note from the outset of the discussion the range of terminology used. Although this paper has chosen to use the phrase data aggregators, others use phrases and words such as data brokers, automated decision making, Big Data, algorithms, artificial intelligence, predictive analysis and profiling, to name a handful.

The facts of *Spokeo Inc v Robins* are useful to consider. The case concerns Mr Thomas Robins, with whom others have joined in a class action against Spokeo Incorporated at a federal level.[2] Spokeo operates a "people search engine",[3] which aggregates data from publicly available sources including public directories, online sources, promotional networks and social media.[4] This website allows people seeking information about another person to find what they are looking for. It is aimed at employers and others conducting searches into the background of individuals.[5] Mr Robins complains about inaccurate information about him on the Spokeo website,

2 *Spokeo Inc v Robins* 136 S Ct 1540 (2016) [*Spokeo*] at 1543.
3 At 1543.
4 Brief for Petitioner *Spokeo Inc v Robins* 2015 WL 4148655 (2015) at 7.
5 *Spokeo*, above n 2, at 1543.

and (with others) has started class action proceedings to vindicate his rights under the Fair Credit Reporting Act 1970.[6] This Act requires credit reporting agencies to "follow reasonable procedures to assure maximum possible accuracy"[7] of consumer reports and it imposes "civil liability for wilful non-compliance".[8] Mr Robins claims that Spokeo generated an inaccurate profile about him; namely that he held a graduate degree, that he was married, in his 50s, employed in a professional field, with very strong economic health and wealth indicators.[9] This inaccurate profile was being displayed while Mr Robins was unemployed, which is alleged to have harmed his employment opportunities.[10]Justice Thomas summarised the conclusion of the majority opinion of the Supreme Court as thus:[11]

> Robins has no standing to sue Spokeo, in his own name, for violations of the duties that Spokeo owes to the public collectively absent some showing that he has suffered concrete and particular harm.

A reader may ask, what is the relevance of the *Spokeo* case to New Zealand? The answer is that there is no direct relevance because the systems of law are different. This is because the *Spokeo* case concerns an American Constitutional doctrine called standing. However, New Zealand does not have a written constitution and instead has a system of parliamentary sovereignty where Parliament is supreme. America's all-encompassing constitution affects everything from their constitutional law to data privacy law. Despite these fundamental differences, both legal systems have to tackle polycentric policy issues, the fundamental problem of scarcity of resources, and the issue of balancing the competing interests of various stakeholders. Equally, both legal systems create ways to limit and prescribe access to justice through courts and tribunals. Article III standing is simply a way of respecting the constitutional doctrine of separation of powers. Similarly, the Privacy Act 2020 also serves a gatekeeping function through the harm requirement. The other aspect of the *Spokeo* case is the legal reasoning used by the majority. There is a similarity with some of the New Zealand jurisprudence in the way legal reasoning is used to obfuscate the vindication of privacy rights.

A reader may ask, why should the law care about data aggregators at all? Data aggregators, under the status quo, threaten the right to informational self-

6 The Fair Credit Reporting Act 1970 (US).
7 At 15 USC § 1681e(b)
8 At 15 USC § 1681n(a).
9 *Spokeo*, above n 2, at 1554.
10 At 1554.
11 At 1553.

determination. The development of notions of informational self-determination underscores vast and innumerable changes in the technological landscape of the last four decades.[12] The invention of the internet, the arrival of smartphones, apps, wearables and developments in metadata technologies; these all signal cultural and environmental change.[13] The critical case on the right to informational self-determination is found in the German Census Act.[14] Eva Fialová describes the approach of the German Federal Constitutional Court to this right, conceiving of it as a "... personality right, which ensures the individual the right to control the issuing and utilization of the personal data".[15] Informational self-determination essentially encompasses "... the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[16] Although there is no particular legal pronouncement on the question, either by statute or case law, the issue is not ignored. The privacy issues posed by data aggregation fall within the wider umbrella of systemic harms. In a recent review of the Privacy Act 1993, the New Zealand Law Commission made some recommendations to address systemic harms, including providing the Privacy Commissioner with the power to issue compliance notices, and removing the harm threshold for privacy complaints.[17] These recommendations were premised on the notion that: "A system centred on complaints by individuals is not always effective in correcting ongoing problems which may continue to affect others."[18] This article agrees with this statement and adds that the effectiveness of individual litigation is similarly constrained.

The question of what is so specific about data aggregators that demands targeted regulation separate from the status quo is a salient one. Data aggregators and the data privacy issues related to them, or decisions based on their activities, pose significant challenges worthy of targeted regulation. The first of these relates to the nature of data aggregators and their business model. It is important to note that data aggregators process and manipulate information on individuals to predict

12 See generally Herman Tavani "Search Engines and Ethics" in Edward N Zalta (ed) *The Stanford Encyclopedia of Philosophy* (2016, online ed).

13 See generally Daniel J Solove *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, New Haven (Conn), 2007). See also Shoshana Zuboff "Big other: surveillance capitalism and the prospects of an information civilization" (2015) 30 Journal of Information Technology 75 at 75–77. See also Karen Rose, Scott Eldridge and Lyman Chapin "The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World" (October 2015) Internet Society <www.internetsociety.org>.

14 See BVerfGE 65, 1 – Volkszählung, Urt v 15.12.1983.

15 Eva Fialová "Data Portability and Informational Self-Determination" [2014] 8 Masaryk University Journal of Law and Technology 1 at 47.

16 Alan Westin *Privacy & Freedom* (The Bodley Head, London, 1967) at 7.

17 Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123, 2011) at 15 and 179.

18 At 15.

behaviour.[19] By their very nature, data aggregators utilise advanced technology to achieve their ends. A negative consequence of this technology is the "multiplier effect".[20] This means that seemingly innocuous bits of information add up to create an information profile that can be used to evaluate people. Second, in the current economy, it is likely that data aggregators who do operate have substantial market power so targeted regulation is necessary in terms complying with competition law (an issue which is beyond the scope of this paper).[21] Third, the harm created by data aggregators is likely to be much greater and longer-lasting. In addition, the technology available to data aggregators can retain information for much longer periods of time.[22]

Finally, and most importantly, there is a mismatch between the technological capacity of data aggregators and the regulation to which they are subject under the status quo. As the Privacy Commissioner states in his submission to the new Privacy Bill: "The current rights and protections available to New Zealanders are gradually weakening as technology develops."[23] This technological shift encompasses "advanced algorithms and artificial intelligence".[24] The Privacy Commissioner champions the need for "algorithmic transparency",[25] and calls on the government to tackle harm that stems from "automated decision making".[26] The Privacy Commissioner notes that: "While data analytics are not new, the availability of more powerful analytical tools creates a greater capacity to analyse large datasets."[27]Again, harking back to the nature of data aggregators, the Privacy Commissioner notes that:[28]

> Data analytics and automated decision-making often lack transparency and provide no meaningful accountability. Systems may appear objective and yet be subject to in-built bias leading to discrimination. Many algorithmic assessment tools operate as 'black boxes' without transparency. This lack of transparency is compounded when private commercial interests claim trade secrecy over proprietary algorithms

19 New Zealand Council for Civil Liberties, above n 1.
20 New Zealand Council for Civil Liberties, above n 1.
21 New Zealand Council for Civil Liberties, above n 1.
22 Office of the Privacy Commissioner "Submission to the Justice and Electoral Committee on the Privacy Bill" at [7.15].
23 At [7.15].
24 At [7.7].
25 At [1.9 (d)].
26 At [1.9 (d)].
27 At [8.4].
28 At [8.6].

> so that even the agencies using the tools may have little understanding over how they operate.

The Privacy Commissioner also critiques the legal status quo thus:[29]

> The [informational privacy] principles do not directly – or arguably very effectively – address the particular risks and issues created by automated decision-making processes. Nor do they require specific mitigations such as algorithmic transparency.

Equally, the removal of the Public Register Privacy Principles from the Privacy Bill, which became the Privacy Act 2020, creates a grey area in which data aggregators can operate. The Privacy Commissioner supports the approach taken to automated decision making in the European Union`s General Data Protection Regulation (GDPR).

In light of the lessons that can be learned from the United States Supreme Court decision in *Spokeo,* it is argued that prospective data privacy harms related to data aggregators, as identified by the minority in the case, are best addressed through a clear and principled regulatory scheme.[30] There are three key reasons for this. First, individual actions, whether in New Zealand or the United States, will need a causal link to actual harm, which means the harms stemming from data aggregators are likely to remain unaddressed. Second, individual litigation is unlikely to address systemic issues that underpin the conceptual scope of these harms, meaning that the rights of victims of data privacy breaches are not protected. Third, giving a regulator (such as the Privacy Commissioner) power and legislative impetus to address these issues will allow a fairer balance between business efficacy and the right to informational self-determination than is afforded under the status quo in New Zealand. Although, in theory, statutory privacy rights that can be upheld through individual litigation and individually oriented complaints forums can act as a deterrent to companies breaching data privacy principles, these protections are limited due to an inconsistent approach to data aggregators across case law, thus weakening access to genuine justice for victims.

This paper is organised as follows: Part II will discuss some salient contextual questions that support the thesis of this paper. Part IIA answers the question of who data aggregators are. Part IIB highlights the broad nature of harms arising

29 At [8.10].
30 *Spokeo*, above n 2, at 1556.

from data aggregators. Part IIC discusses the relevance of informational privacy principle 8. Part IID discusses the relevance of the Credit Reporting Privacy Code 2004. Part IIE discusses the relevance of New Zealand Privacy jurisprudence. Part III will outline the *Spokeo* decision, including the facts and procedural history. Part IV will examine arguments supporting the regulatory approach. Part IVA will discuss the knowledge gap and how the regulatory route would lead to a more proactive response relating to data privacy concerns stemming from data aggregation. Part IVB outlines the uncertainty about whether a case involving a data aggregator will meet the harm requirement in the Privacy Act 2020. Part IVC showcases the systemic nature of data privacy harms from data aggregators and how a regulatory approach can provide a holistic response. Part IVD underscores how a *sui generis* piece of legislation on data aggregators can allow a new societal consensus to be formed on the issues that strike the appropriate balance between competing interests. Part IVE revisits the argument that a blanket policy of loosening the harm requirement will not necessarily lead to positive outcomes in relation to concerns about data aggregators. It may make it easier for vexatious litigants to abuse the prevailing process that applies to general privacy cases. Part V and VI concludes that in order to address the data privacy concerns of data aggregators, a regulatory model based on a *sui generis* piece of legislation on data aggregators can be useful in bringing New Zealand privacy law into modernity.

II. Context

A. Who are Data Aggregators?

The question of "Who are these data aggregators?" is a difficult one, and the answer is equally complex. The reason for this complexity is the variety of definitions involved, and domain-specific variation in the use of terminology. For example, the definition of Big Data is useful to consider. According to Google, Big Data is defined as the use of "[e]xtremely large datasets that maybe analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions".[31] The New Zealand Privacy Commissioner also canvasses some interesting definitions, which are relevant to consider, namely relating to algorithmic or automated decision making and predictive analytics or predictive risk modelling. Algorithmic or automated decision making is defined as "… tools relying on algorithms, programming or Artificial Intelligence (AI) to assess

31 Google "Definition of Big Data" (31 August 2020) Google Search <www.google.com>.

information and make a decision on outcomes which would formerly have been made by a human".[32] Similarly, predictive analytics or predictive risk modelling is defined as "... a statistical tool that attempts to determine future outcomes or likelihood of risk by analysing the characteristics associated with those outcomes in historical cases".[33] To make matters even more complex, the European Union's GDPR regulates automated decision making and profiling.[34] Interestingly, profiling is a potential aspect of automated decision making.[35] Crucially, the GDPR provides a definition of profiling as:[36]

> [The] automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Despite the varying definitions and terminology relating to data aggregators, common themes emerge across the various definitions. One of the common themes is the type of business model used, which entails compiling and processing available data using technology to map and predict individual behaviour and characteristics.[37] According to United States sources, the aggregation of data about individuals on the internet is an industry worth at least USD 31 billion.[38] Equally, the United States Federal Trade Commission (FTC) uses the term data brokers and notes some key characteristics about them. The FTC notes that the "... data broker industry is complex, with multiple layers of data brokers providing data to each other".[39] The FTC also alleges that "data brokers collect consumer data from numerous sources, largely without consumers' knowledge".[40]

32 Office of the Privacy Commissioner, above n 22, at [8.1 (a)].
33 At [8.1 (b)].
34 At [8.12]
35 At [8.13].
36 Regulation 2016/679 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 L119/1 [GDPR], art 4(4).
37 See generally Thomas C Redman "4 Business Models for the Data Age" (2015) Harv Bus Rev (online ed).
38 JD Sartain "Feds cracks down on data brokers: But protecting your online privacy remains an uphill battle" *Network World* (online ed, 2 July 2012). See generally Anne Branscomb *Who Owns Information?: From Privacy to Public Access* (Basic Books, New York, 1995).
39 Federal Trade Commission *Data Brokers: A Call for Transparency and Accountability* (Federal Trade Commission, May 2014) at iv.
40 At iv.

Beyond the theoretical definitions of data aggregators, it is important to answer the question: who these data aggregators are, and whether they operate in New Zealand. Data aggregators (including those that fit related and intersecting definitions) are varied. As far as the *Spokeo* case is concerned, there were companies that signed a brief of Amicus Curiae in support of Spokeo, who stood against the Ninth Circuit's Approach to art III standing. These companies include Google, Yahoo, Twitter, LinkedIn and Netflix.[41] Google and Facebook are arguably data aggregators, fitting some of the varied and intersecting definitions; but each with its own unique business model. As far as whether data aggregators operate in New Zealand, this is a difficult question as it depends on how data aggregators are defined. A 2012 New Zealand Herald article states that data brokers operate in New Zealand. According to this article, Acxion, one of the world's largest data brokers, has a New Zealand office in Auckland Central.[42] It also mentions New Zealand Post's Genius segmentation tool "which enables household profiling by income and ethnicity".[43] It also cites another data broker, Mosaic NZ, "... which uses data from the Census, QV, Land Information New Zealand and surveys conducted by the Roy Morgan market research company".[44] Interestingly, these data brokers have a variety of clients, including corporates and NGOs such as the Fred Hollows Foundation.[45] Even if one assumes there are no data aggregators currently operating in New Zealand, the removal of the Public Register Privacy Principles from the Privacy Bill that formed the Privacy Act 2020 also creates a loophole those data aggregators could exploit to operate in the future.[46]

B. What is the Nature of Harms arising from Data Aggregators?

The nature of harms arising from data aggregators is broad and is not confined to inaccurate records kept by data aggregators, as demonstrated in the *Spokeo* case. Equally, these broad ranges of harms are interconnected and some types of harms, such as inaccuracy, can have more pernicious effects. In the end, all the various harms act in concert to have an overall negative effect. The champions of

41 Matthew S De Luca "The Hunt for Privacy Harms After Spokeo" [2018] 86 Fordham L Rev 2439 at 2456.

42 Nicholas Jones "For sale: your private details" The New Zealand Herald (online ed, Auckland, 26 September 2012).

43 Jones, above n 42.

44 Jones, above n 42.

45 Jones, above n 42.

46 See generally Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, 2008) at 6–7 and 12–13.

informational self-determination would support consideration of the broad harms of data aggregators in a holistic manner.

It is argued that there are two main harms, from which all other harms stem. First, having inaccurate records or inaccurate information about a person. Second, having information that is out of date and should be deleted as the advocates of the 'right to be forgotten' require[47] and as occurs in the European GDPR.

If one looks at this issue in terms of the informational privacy principles, data aggregators are likely to breach these principles, especially if they all conduct themselves in the manner that Spokeo did, in particular, informational privacy principles 7, 8 and 9. Principle 7 entitles an individual to request a correction of information. Principle 8 enshrines the need for information to be accurate and up to date. Principle 9 notes that an agency must not keep information longer than necessary for the purpose for which it was collected.

American legal scholars, such as Matthew De Luca, argue:[48]

> [T]he law has not yet fully developed to recognize the concrete privacy harms that can result from what otherwise seems like ordinary economic activity involving the widespread aggregation and compilation of data.

It is important to note that data aggregators are not a monolith; they are diverse, and this also impacts on the nature of harm.

Inaccurate records of information can have very tangible impacts such as the loss of a credit rating. The loss of a credit rating would count as a loss of benefit for which damages would be awarded in the HRRT.[49] Another way to conceptualise the harm stemming from data aggregators is to draw parallels from harms that stem from the operation of public registers. The link between data aggregators and public registers is founded upon public registers being the most common source of publicly available and accessible information for data aggregators. Equally, there is also a parallel with the diverse nature of public registers and the diverse nature of data aggregators. It is thus relevant to consider some of the harms that stem from public registers as outlined by the Law Commission. These harms include a "… spectre of criminal activity resulting from accessing and aggregating personal information from registers".[50] The possible criminal activities include stalking, harassment, theft

47 See Amanda Cheng "Forget About the Right to be Forgotten: How About a Right to be Different?" (2016) 22 Auckland U L Rev 106 at 141.
48 De Luca, above n 41, at 2439.
49 See *Director of Human Rights Proceedings v Hamilton* [2012] NZHRRT 24 at [84].
50 Law Commission, above n 46, at 66.

and identity crime.[51] Although the harms from public registers and data aggregators are not exactly the same, they are relevant to considering the question of how data aggregators collect data and the role of permission.[52] The Privacy Commissioner also warns that:[53]

> [T]he requirement in principle 9 for information to be kept for no longer than is necessary is rendered meaningless in the context of advanced algorithms and artificial intelligence. For example, the thirst of artificial intelligence systems for data will mean that agencies will want to keep all of the data that is available for increasing periods of time.

The issue of stale data being retained can have serious consequences. For example, an old address can be used by thieves to guess passwords and challenge questions.[54] There is also a growing scholarship, particularly in America, around the risks of discrimination including racial discrimination, posed by data aggregators.[55] Māori have increasingly called for Māori data sovereignty to be recognised and Te Tiriti O Waitangi to be honoured with respect to Big Data.[56]

C. What is the Relevance of Informational Privacy Principle 8 on Data Accuracy to the Discussion about Data Aggregation?

The informational privacy principle 8 of the Privacy Act 2020 is relevant to this discussion about the regulation of data aggregators in relation to prospective privacy harms. Information Privacy Principle 8 provides that:[57]

> An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

51 At 66.
52 Federal Trade Commission, above n 39, at 3.
53 Office of the Privacy commissioner, above n 22, at [7.15].
54 Federal Trade Commission, above n 39, at
55 At 56.
56 See generally Tahu Kukutai and John Taylor "Data sovereignty for indigenous peoples: current practice and future needs" in Tahu Kukutai and John Taylor (eds) *Indigenous Data Sovereignty: Toward an Agenda* 1 at 1–25.
57 Privacy Act 2020, s 22.

The crux of the issue is as follows: if data aggregators are collecting and disclosing inaccurate information, then it is possible to argue that it is covered by principle 8. However, if a data aggregator is using the information to generate some type of score or evaluation, such as whether a person is generally truthful, wealthy or trustworthy, it is less arguable whether it is caught by principle 8.

In *Taylor v Orcon*, there were serious delays in rectifying a disputed debt which resulted in a negative credit rating for the claimants. In *Taylor v Orcon*, the HRRT notes that:[58]

> The language of Principle 8 makes it clear that the more serious the potential consequences of using the personal information held by the agency, the greater the degree of care which must be exercised before the information is used.

Equally, the HRRT held that "'Reasonableness' in Principle 8 includes timeliness".[59] Assuming data aggregators are covered by principle 8, then these obligations will give protection to claimants similar to that in the *Spokeo* case. However, this is not the end of the matter. In order to receive any privacy law remedy in New Zealand, the issue of harm must be resolved.

D. What is the relevance of the Credit Reporting Privacy Code 2004 in the discussion of Data Aggregators in New Zealand?

Admittedly, the question of the relevance of the Credit Reporting Privacy Code 2004 to this discussion about the regulation of data aggregators with respect to data privacy issues is a difficult one. This is because, first, such a case testing the relevance has neither come before the HRRT nor the New Zealand courts. Second, as the HRRT noted in *Taylor v Orcon*, the Credit Reporting Privacy Code 2004 encourages "an ex post facto exercise".[60] This means that even if the Credit Reporting Privacy Code 2004 applies, its application will not provide much solace to the victim as their credit rating would already be damaged, since the victim would have only just become aware of the negative credit rating due to delays associated with the nature of data aggregators. Third, the Credit Reporting Privacy Code 2004, like the Privacy legislation, was not designed with data aggregators in mind, so if it does apply, it could only apply in a narrow way. The issue of whether the

58 *Taylor v Orcon* [2015] NZHRRT 15 at [46].
59 At [84].
60 At [44].

Credit Reporting Privacy Code 2004 will apply to data aggregators will depend on how credit information is defined. If it does apply, there would be onerous duties imposed on data aggregators.[61] Even if it does apply, the Credit Reporting Privacy Code 2004 would be classed as secondary or delegated legislation. Thus, it would have an inferior status to statutory legislation on account of being struck down by the courts. The issue becomes difficult because some well-known credit reporters such as Veda or Astricx are solidly regulated by the Code. Nevertheless, banks may wish to go beyond these and consult data aggregators with data warehouses of information to figure out consumer buying habits. There is a grey area here which creates the problem. Ultimately, if the Credit Reporting Privacy Code is supposed to regulate the actions of data aggregators, it is not fit for purpose, and it needs a holistic revision in this respect.

E. The Relevance of New Zealand Data Privacy Law Jurisprudence

It is important to consider the impact of New Zealand privacy jurisprudence on cases relating to prospective privacy harms that stem from data aggregators. There has not been a case of data aggregators which tests the data privacy harms in the HRRT or the courts yet. Thus, one is limited to seeing how the New Zealand legal system works for 'run of the mill' privacy cases (which do not involve the varied and intersecting definitions related to data aggregators) and then extrapolating from those cases to discuss hypothetical outcomes for cases involving data aggregators. In addition, Rodger Haines QC notes a salient point, namely:[62]

> The Privacy Act has been in force for 24 years. As with the associated Human Rights Act, there has never been a comprehensive review at senior court level of principles engaged when awarding damages under the common provisions that compensate for pecuniary loss, loss of benefits, humiliation, loss of dignity and injury to feelings.

61 See Credit Reporting Privacy Code 2004, cl 6 rr 6–11.

62 Rodger Haines "Damages for Interference with Privacy Under Statute: The New Zealand Privacy Act 1993" in Jason NE Varuhas and NA Moreham (eds) *Remedies for Breach of Privacy* (Hart Publishing PLC, Oxford, 2018) 349 at 374–375.

Varuhas and Moreham note "… privacy is not an island: the field lies at the intersection of several areas of law, including torts, equity and human rights".[63] Also as a comment on the general privacy law field, they note:[64]

> The remedial principles in the new field of privacy are not well-established and in general have not been the subject of extended treatment either in intermediate or apex courts or in scholarly work.

Associate Professor Gehan Gunasekera also notes that:[65]

> It is 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.

Let us assume that an inaccurate data profile created by a data aggregator does not lead to any loss of benefit but does lead to some emotional harm. The sticking point then becomes establishing emotional harm. This is a subjective issue. In *Hammond*, the Tribunal noted a quote from a United Kingdom case, namely that: "translating hurt feelings into hard currency is bound to be an artificial exercise".[66] Equally, in a discussion of the Australian data privacy law framework, Norman Witzleb comments:[67]

> 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.

63 Jason NE Varuhas and NA Moreham "Remedies for Breach of Privacy" in Jason NE Varuhas and NA Moreham (eds) *Remedies for Breach of Privacy* (Hart Publishing PLC, Oxford, 2018) 1 at 2.

64 At 3.

65 Gehan Gunasekara "Enforcement Design for Data Privacy: A Comparative Study" Sing JLS (forthcoming) at 2.

66 *Hammond v Credit Union Baywide* [2015] NZHRRT 6 at [170.7] (footnote omitted).

67 Norman Witzleb "Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy" in J Varuhas and N Moreham (eds) *Remedies for Breach of Privacy* (Hart Publishing PLC, Great Britain, 2018) 377 at 393.

These conclusions set up the context that is a perfect storm for negative issues that relate to data aggregators.

One of the relevant aspects relates to the adequacy of damages for breaches of privacy. In the *Hammond* case, the HRRT noted that:[68]

> The award of damages is to compensate for humiliation, loss of dignity and injury to feelings, not to punish the defendant. The conduct of the defendant may, however, exacerbate (or, as the case may be, mitigate) the humiliation, loss of dignity or injury to feelings and therefore be a relevant factor in the assessment of the quantum of damages to be awarded for the humiliation, loss of dignity or injury to feelings.

This seemingly benign quote from the *Hammond* case is of great importance for understanding the contradictions of the current privacy law system and will be directly relevant to the following discussion of the cases relating to Mr Kim Dotcom. Equally, Mr Haines notes that:[69]

> The Tribunal's power to award damages is entirely statute-conferred. Each of the three permitted categories of damages is overtly compensatory in nature. No express provision made for the award of damages for a wrongful interference with privacy where no loss or harm of the kind recognised in section 88(1) has occurred. On conventional principles of statutory interpretation it would be difficult to award exemplary damages, particularly when of the three statutes under which the Tribunal has jurisdiction to award damages, only the Health and Disability Commissioner Act makes provision for the award of such damages.

Mr Haines states that:[70]

68 *Hammond,* above n 66, at [170].

69 At 365.

70 At 365. See also *Winter v Jans* HC Hamilton CIV-2003-419-854, 6 April 2004 [*Winter*] at [54]; and *Chief Executive of the Ministry of Social Development v Holmes* [2013] NZHC 672, [2013] NZAR 760 (HC) [Holmes] at [140].

> The view foreshadowed by the High Court in *Winter v Jans* and adopted by the New Zealand Law Commission is that a distinct punitive element is not required because the motives and conduct of the defendant are to be taken into account in the context of section 85(4), which provides that while it is not a defence that the interference with privacy was unintentional or without negligence on the part of the defendant, the Tribunal must take the conduct of the defendant into account in deciding what, if any, remedy to grant.

The *Dotcom* saga, especially in terms of the differential approach of the HRRT and the High Court, demonstrates the fallibility of the existing privacy law framework in regard to how it impacts data aggregators. There is an interesting nuance in the *Dotcom* case because it involves the notion that "hard cases make bad law". However, it is argued that hard cases, in fact, show bad law or the bad application of the law. Thus, it is pertinent to consider the facts of the *Dotcom* case. Mr Kim Dotcom made 52 requests to all the Ministers of the Crown and a majority of government departments.[71] These requested all personal information held about him and this request was tagged with urgency due to his pending legal action.[72] These requests were transferred to the Attorney General,[73] who declined them on the ground that they were vexatious and trivial as per s 29(1) of the Privacy Act.[74] It is now important to turn to the gulf between the approach of HRRT and High Court in the *Dotcom* case. The HRRT in the *Dotcom* case held that:[75]

> We have found the Crown to be in clear breach of its obligations under the Privacy Act. There has been no breach of standards by Mr Dotcom and in any event there is a very high threshold for exception. There is no disentitling conduct to deny Mr Dotcom expression of the findings made by the Tribunal in the form of a formal declaration.

The approach of the High Court in the *Dotcom* case was very different from that of the HRRT. In order to understand the overall approach of the High Court, it is important to understand how the court viewed the operation of the Privacy Act.

71 *Dotcom v Crown Law Office* [2018] NZHRRT 7 at [1].
72 At [1].
73 At [2].
74 At [3].
75 At [217].

Justice Churchman preferred the characterisation of the foundations of the Privacy Act as being "principles-based and open textured, and regulat[ing] in a rather light-handed way".[76] The Court also referred verbatim from the Law Commission report, which noted:[77]

> Rather than setting out strict rules about how personal information may be handled, the Act is based on a set of 12 privacy principles. These principles provide agencies with a high degree of flexibility in terms of how they comply with them.

Judge Churchman characterised Mr Dotcom's request as an "everything request".[78] The High Court makes an analogy with employment jurisprudence to support the need for the claimant to provide evidence for damages under humiliation, loss of dignity and injury to feelings grounds. [79] Despite the High Court accepting the approach to damages in the Hammond case, the Court nonetheless notes the errors of the Tribunal's approach, namely:[80]

> [T]here is little analysis of the specific effect on Mr Dotcom. The obvious reason for that is that, in relation to this particular request, he gave no evidence at all as to its effect on him. He certainly did not claim that its effect had been "stigmatising" as the HRRT concluded.

It is argued that the High Court utilises strained reasoning to deny Mr Dotcom a remedy. Although not explicitly mentioned, this may be due to Mr Dotcom's unusual manner. Nonetheless, the law was sufficiently malleable for judicial reasoning to provide him with a remedy, although it did not eventuate. Another bulwark which the High Court relied upon to deny Mr Dotcom a remedy is an aforementioned notion that HRRT damages are compensatory and not for the punishment of the defendant. Even if one accepts this as the statement of how the law currently stands, it does not stop calls for law reform, especially considering the impact of this legal status quo on claimants who face privacy harm from data aggregators. Also, there are two separate issues operating here: first, what the data privacy law should generally be,

76 *Attorney-General v Dotcom* [2018] NZHC 2564 [*Dotcom*] at [8] (footnote omitted).
77 At [8] (footnote omitted).
78 At [10].
79 At [227] and [228].
80 At [230].

and second, what data privacy law should be for data aggregators. There may be compelling policy reasons to retain the status quo for general data privacy cases. However, the status quo simply does not work for cases involving data aggregators. Also, instead of a judge having to use strained reasoning to justify damages, why not give a clear legislative impetus for vindication? The advantages of such legislation especially apply in the case of data aggregators, where the imbalance between the claimant and the data agency is so vast.

III. Spokeo Decision

A. Procedural History of Spokeo Inc v Robins

1. United States District Court Central California Decision

This case initially started at the United States District Court, where Spokeo attempted to dismiss Mr Robins' First Amended Complaint, after the District Court denied Mr Robins' complaint and gave him 20 days to amend it. [81] Mr Robins alleged "… actual and/or imminent harm by creating, displaying, and marketing inaccurate consumer reporting information about the Plaintiff".[82] Judge Otis D Wright II found that Mr Robins allegations are "… sufficient to support a plausible inference that Defendant's conduct falls within the scope of the FCRA".[83] The court further declined to dismiss Spokeo's argument based on immunity under the Communications Decency Act and it declined Mr Robins' claim based on unfair competition.[84] The court granted Spokeo's motion to dismiss in part and denied it in part.[85]

2. Ninth Circuit Court of Appeals' decision

Judge O'Scannlain of the Ninth Circuit posed the legal issue as: whether Mr Robins had art III standing to sue Spokeo (via the FCRA) for creating an inaccurate profile of information about Mr Robins on their database.[86] The court notes that the District Court correctly identified the components of standing, which include:[87]

81 *Robins v Spokeo Inc* No. CV10-05306 ODW (AGRx) WL 1793334 (CD Cal May 11 2011) at 1.
82 At 1.
83 At 2.
84 At 3.
85 At 3.
86 *Robins v Spokeo Inc* 742 F 3d 409 (9th Cir 2014) at 410.
87 At 412 (footnote omitted).

(1) The plaintiff "had suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical";
(2) "the injury is fairly traceable to the challenged to the challenged action of the defendant"; and
(3) "it is likely, as opposed to merely speculative, that the injury will be redressed by a favourable decision."

The court starts with a discussion of two fundamental tenets relating to standing and statutory rights, firstly that "Congress's creation of a private cause of action to enforce a statutory provision implies that Congress intended the enforceable provision to create a statutory right"[88] and secondly the "... violation of a statutory right is usually a sufficient injury in fact to confer standing."[89]Although the Ninth Circuit does reiterate the importance of the constitutional imperatives that underlie the law of standing and the concern to limit "... the power of Congress to confer standing"[90], it nonetheless ruled that these constitutional concerns do not prevent Congress from recognising new injuries that would have previously not met the standing requirements.[91] Therefore Justice O'Scannlain poses the central issue before the court as "... whether violations of statutory rights created by the FCRA are "concrete, defacto injuries" that Congress can so elevate".[92] To illustrate the solution to the issue posed, the court made the analogy to the approach of the Sixth Circuit in *Beaudry v Telecheck Services Inc*.[93] This case considered whether a breach of the FCRA is sufficient to constitute standing to sue (namely an injury-in-fact) under the civil liability provisions of the FCRA.[94] The civil liability provision states:[95]

> *In general*. Any person who wilfully fails to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer in an amount equal to the sum of
>
> (1) (A) any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000; or

88 At 412.
89 At 412.
90 At 413.
91 At 413.
92 At 413.
93 *Beaudry v Telecheck Services Inc* 579 F 3d 702 (6th Cir 2009).
94 At 707.
95 At 15 USC § 1681n(a).

> (B) in the case of liability of a natural person for obtaining a consumer report under false pretenses or knowingly without a permissible purpose, actual damages sustained by the consumer as a result of the failure or $1,000, whichever is greater;
> (2) such amount of punitive damages as the court may allow; and
> (3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

This case set the constitutional parameters of standing, requiring that:[96]

> First, a plaintiff "must be 'among the injured,' in the sense that she alleges the defendants violated her statutory rights". Second, the statutory right at issue must protect against "individual, rather than collective, harm."

The Ninth Circuit affirms that Mr Robins' case fell within this rubric and held that "Robins' personal interest in the handling of his credit information are individualized rather than collective".[97] Ultimately the Court affirmed that "... alleged violations of Robins' statutory rights are sufficient to satisfy the injury-in-fact requirement of Article III".[98]

3. Spokeo Inc v Robins Decision in the Supreme Court

(a) Majority decision

(i) Justice Alito's judgment

The decision of Ninth Circuit was appealed, and Justice Alito, for the majority, started with critiquing the approach of the Ninth Circuit on the law of standing. Justice Alito found that the Ninth Circuit erred by not utilising both parts of the dual-pronged test for injury-in-fact laid out earlier by the Supreme Court in *Friends of the Earth Inc v Laidlaw Environmental Services (TOC).*[99] Namely, the Ninth Circuit

96 *Robins v Spokeo Inc,* above n 86, at 413.
97 At 413.
98 At 413–414.
99 *Spokeo Inc v Robins*, above n 2, at 1545. See also *Friends of the Earth Inc v Laidlaw Environmental Services (TOC) Inc,* 528 US 167, 180–181, 120 S Sct 693, 145 Led2d 610 (2000).

should have considered both concreteness and particularity. In fact, the Ninth Circuit recognised particularity alone, and ignored concreteness. Therefore, the Ninth Circuit decision was vacated and the Ninth Circuit was ordered to conduct the full analysis.

In terms of Justice Alito's legal reasoning, there is an air of suspicion of Mr Robins as a bona fide plaintiff, perhaps because this case underpins a class action. This is particularly seen in the following verbatim:[100]

> At some point in time, *someone (Robins' complaint does not specify who)* made a Spokeo search request for information about Robins, and Spokeo trawled its sources and generated a profile. *By some means not detailed in Robins' complaint,* he became aware of the contents of that profile and discovered that it contained inaccurate information.

Furthermore, Justice Alito's judgment focuses strongly on the constitutional role of the United States' law of standing and its particular doctrinal relation to the separation of powers.[101] In attacking the reasoning of the Ninth Circuit, Judge Alito noted that: "Particularization is necessary to establish injury in fact, but it is not sufficient … An injury in fact must also be 'concrete'."[102] Such an injury "… must be 'defacto'; that is, it must actually exist".[103] However, Justice Alito is quick to note that: "'Concrete' is not, however, necessarily synonymous with 'tangible'."[104]

Justice Alito highlights a tension in the law and then takes a particular side. On the one hand, Justice Alito suggests that Congress may "… elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law".[105] On the other hand, Justice Alito finds that:[106]

> Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to vindicate that right.

100 *Spokeo,* above n 2, at 1546 (emphasis added).
101 At 1547–1548. See also United States Constitution, art 3.
102 At 1548.
103 At 1548.
104 At 1549.
105 *Lujan v Defenders of Wildlife* 504 US 555 (1992) at 578.
106 *Spokeo*, above n 2, at 1549.

Again, Justice Alito put forward another contingency to his articulation of the law, namely that it "… does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness".[107] Justice Alito's overall conclusion in this matter captured the main tension present throughout the case. Justice Alito found that Congress intended to stop the spread of inaccurate information profiles through the measures outlined in the FCRA.[108] Equally, Justice Alito emphasises that a "bare procedural violation" will not meet the standing requirements, because such violations "… may result in no harm".[109] Justice Alito provides the example of the credit reporter who fails to meet the requirement to provide notice, despite the information on the credit reporter's database being entirely correct.[110] Further Justice Alito finds that "… not all inaccuracies cause harm or present any material risk of harm" and provides the example of an inaccurate zip code.[111] Ultimately Judge Alito ordered a vacation of the Court of Appeal's judgment.[112]

(ii) Justice Thomas' judgment

Justice Thomas' judgment concurred with Justice Alito's judgment and formed the majority approach.[113] The nuance of Justice Thomas's reasoning lies in how he conceptualises the relationship between the law of standing and different categories of rights.[114] In canvassing the history of the common law, Justice Thomas notes a salient trend where the role of the courts in redressing of a public right is heavily circumscribed as compared to private rights.[115] Private rights claims brought by individuals are more readily adjudicated.[116] This trend is said to persist in the current formulation of standing.[117] Justice Thomas emphasises the distinction between the vindication of private rights and public rights in his reasoning.[118] This trend originated because the state was granted the sole role of taking legal action to redress breaches of public rights through the mechanism of the criminal law.[119] In the unusual situation where individuals sought to vindicate public rights, they had to prove that the "… violation caused them 'some extraordinary damage, beyond the rest of the [community]'".[120] According to Justice Thomas "… standing

107 At 1549.
108 At 1550.
109 At 1550.
110 At 1550.
111 At 1550.
112 At 1550.
113 At 1550.
114 At 1550.
115 At 1550.
116 At 1550.
117 At 1550.
118 At 1551.
119 At 1551.
120 At 1551.

doctrine keeps courts out of political disputes by denying private litigants the right to test the abstract legality of government action".[121] Equally a private individual attempting to bring a case based on a public right found in a Federal statute "... must demonstrate that violation of that public right has caused him a concrete, individual harm distinct from the general population".[122] In applying this logic, Justice Thomas concluded that:[123]

> The Fair Credit Reporting Act creates a series of regulatory duties. Robins has no standing to sue Spokeo, in his own name, for violations of the duties that Spokeo owes to the public collectively absent some showing that he has suffered concrete and particular harm.

(b) Minority Approach

Justice Ginsburg delivered the minority judgment to which Justice Sotomayor joined.[124] Justice Ginsburg's judgment is consistent with the majority approach regarding the constitutional principles related to the law of standing.[125] However, the reasoning soon starts to diverge. Justice Ginsburg doubted the need for a remand on the matter of whether the "concreteness" element of the injury-in-fact inquiry had been met.[126] Justice Ginsburg opined that Mr Robins' case had fully met the concreteness requirement.[127] Justice Ginsburg outlines that:[128]

> The Court`s opinion observes that time and again, our decisions have coupled the words "concrete *and* particularized." ... True, but true too, in the four cases cited by the Court, and many others, opinions do not discuss the separate offices of the terms "concrete" and "particularized".

Justice Ginsburg asserts that Mr Robins' claim is not one related to the "public at large".[129] In fact, Mr Robins "... seeks redress not for harm to citizenry, but for Spokeo's spread of misinformation specifically about him".[130]

121 At 1552.
122 At 1553.
123 At 1553.
124 At 1554. See also *Federal Election Commission v Akins* 524 US 11(1998) at 19–20.
125 At 1554.
126 At 1555.
127 At 1555.
128 At 1555 (emphasis added).
129 At 1555.
130 At 1555.

Unlike the majority, Justice Ginsburg identifies some concrete harms that pertain to Mr Robins. Justice Ginsburg notes:[131]

> Far from an incorrect zip code, Robins complains of misinformation about his education, family situation, and economic status, inaccurate representation that could affect his fortune in the job market.

Justice Ginsburg concludes by challenging the need for the Ninth Circuit to revisit the matter of concreteness of harm, which is found to be manifest in the evidence put before the Court thus far.[132]

IV. The Case for a Regulatory Approach

A. The Knowledge Gap and how the Regulatory Approach would be more Proactive

In seeking justice for victims of data privacy harms by data aggregators, a regulatory approach would be more proactive because of the operation of the "knowledge gap" in relation to data collection, data privacy law and ability to identify that there has been a breach of a data privacy principle.[133] The regulatory approach would take account of the knowledge gap by forming a safety net, notwithstanding an individual's level of knowledge of their data privacy situation. There would be no need to wait for a case to be brought. Professor Paul Schwartz notes the power imbalance and asymmetry of knowledge between everyday people and data aggregators that highlight this knowledge gap.[134]

The knowledge gap poses a problem to data privacy law's handling of cases involving data aggregators through the operation of delays. If individuals do not know that a data aggregator holds information about them, how could they know whether or not it is incorrect and how could they request a correction? The effect of delays in either reducing damages,[135] or rendering the case to have no remedies,[136] is seen in the Human Rights Review Tribunal case law. In *Deeming*, the

131 At 1556.
132 At 1556.
133 Paul M Schwartz "Privacy and Democracy in Cyberspace" (1999) 52 Vand L Rev 1609 at 1683.
134 At 1683.
135 *Deeming v Whangarei District Council* [2015] NZHRRT 55 at [81]. See also *Te Wini v Askelund* [2015] NZHRRT 21 at [47]–[49].
136 *Sansom v Chief Executive, Department of Internal Affairs* [2016] NZHRRT 17 at [44].

Tribunal found in favour of Mr Deeming's case about breach of privacy principle 11 by the Whangārei District Council and the Tribunal made an award of NZD 2,000 for humiliation, loss of dignity and injury to feelings.[137] However, this was a far cry from the NZD 40,000 Mr Deeming sought for humiliation, loss of dignity and injury to feelings; and the NZD 10,000 sought for aggravated damages.[138] The delay of six years in bringing a claim, and the parallel disclosure to the Northland Rugby Union, were the key factors for the Tribunal granting a reduced level of award.[139] Equally, in *Sansom*, the Tribunal dismissed Ms Sansom's claims for damages,[140] although a declaration of a breach was given, on the reasoning that:[141]

> The basic flaw in Ms Sansom's case is that the harm about which she complains and for which she seeks a remedy flows from events which occurred in late 2010 and the first half of 2011 when she was employed by the Department, not from the Department's failure nearly two years later to comply with its obligations under the Privacy Act.

Hypothetically, if there were any privacy breaches while Ms Sansom was employed, she could have complained about it without delay at the time she was working in the Department. The examples of *Deeming* and *Sansom* show the pernicious effect of delays on the success of data privacy cases in the HRRT and thus one must grapple with the reality that the delays will be worse for those involving data aggregators.

Certainly, assuming that status quo will work for data aggregators will not be proactive. There would need to be a proper mandate that would establish checks and balances so that possible risks could be addressed. The proper mandate should come from a legislative impetus. Some may say that a notion of a knowledge gap is overstated, and perhaps does not give credit to the increasingly knowledge-savvy public. There is truth to this, and some gaps in knowledge can be corrected through legal assistance, as in the case of *Director of Human Rights Proceedings v Valli*,[142] where the request for information was made with the help of the Community Law Centre.[143] However, the knowledge gap remains a systemic problem. It lies in the continual deference to the notion of "Industry Knows Best".[144] Tighter regulation on

137 *Deeming*, above n 135, at [67] and [84.2].
138 At [79].
139 At [72]–[73] and [83].
140 *Sansom*, above n 136, at [59].
141 At [44]
142 *Director of Human Rights Proceedings v Valli* [2014] NZHRRT 58.
143 At [19].
144 Schwartz, above n 133, at 1687.

data aggregators, in addition to the New Zealand privacy complaints system, can make this system more effective for those it serves by buffering the effects of the knowledge gap and consequently minimising the need for long litigation. It would also reduce delay, leading to likely greater awards of damages.

B. Uncertainty about meeting the Harm Requirement

If a case similar to *Spokeo* were to arise in New Zealand, it is uncertain whether the victim would be able to meet the harm requirement under s 66 of the Privacy Act 2020.[145] The provision states than an action is only considered an interference with the privacy of an individual, if the Privacy Commissioner or the pertinent tribunal considers that the action:[146]

> (i) has caused, or may cause, loss, detriment, damage, or injury to that individual; or
> (ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or
> (iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.

As Professor Daniel Solove states: "Most privacy problems lack dead bodies."[147] Therefore, the focus in tackling the challenges brought on by data aggregators should be addressed through targeted legislation. Although, in theory, the harm required could be met and the plaintiff could get some recourse, in practice, there are several limiting factors to be considered. First, s 14(a) of the Privacy Act outlines that the Privacy Commissioner shall:[148]

> ... have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.

145 Privacy Act 1993, s 66.
146 At s 66(1)b.
147 Daniel J Solove '"I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego L Rev 745 at 768
148 Privacy Act 2020, s 14(a).

This provides an interpretive aid for the Privacy Commissioner in balancing competing interests. It appears to invite the Commissioner to weigh the interests of the data aggregators against those of victims of data privacy harms and not to concentrate solely on the victims. Second, as per the Interpretation Act 1999: "The meaning of an enactment must be ascertained from its text and in the light of its purpose."[149] Although the text remains relatively hopeful, the stated purpose of the enactment sends mixed signals. The purpose of the Act is not only about human rights but also about business imperatives and efficiency and how these can be balanced in some happy marriage. A sign of this is seen in the long title of the Privacy Act 2020 which refers to the OECD Guidelines Governing the Protection of Privacy and Trans-border flows of personal data.[150] Associate Professor Stephen Penk contends that:[151]

> It would therefore be a mistake to see the Act as purely a human rights statue and a freedom of information statute. It also has, in its insistence on conformity with the OECD Guidelines, the purpose of facilitating data flows thereby enhancing both government and business efficiency.

In a similar vein, Minister of Justice, Hon D.A.M. Graham, on the third reading of the Privacy Bill stated that: "This legislation is a persuasive type of legislation, rather like the human rights laws. It's not meant to be punitive." [152] Arguably, the New Zealand Privacy Act fits what Harvard law professor Cass Sunstein calls an "incompletely theorized agreement".[153] This is a compact that is vague and logically inconsistent, created deliberately to enable peoples from divergent perspectives to reach an agreement on a contested legal matter.[154]

Third, in meeting the causation requirement that factors into the harm requirement, the prevalence of other causal factors leading to harm (apart from causal factors related to the defendant) often leads to a lack of a remedy. Essentially, data privacy harms (including those involving data aggregators) do not exist in a vacuum and often involve a complex factual matrix. This is seen in cases such as *Balfour v Attorney General*.[155] In *Balfour*, the Court found that there were other factors

149 Interpretation Act 1999, s 5(1).
150 Privacy Act 2020, long title.
151 Stephen Penk "The Privacy Act 1993" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (Brookers Ltd, Wellington, 2010) 49 at 54–55.
152 (5 May 1993) 535 NZPD 15210.
153 Cass Sunstein "Incompletely Theorized Agreements"108(7) Harv L Rev 1733 at 1735.
154 At 1735.
155 *Balfour v Attorney-General* [1991] 1 NZLR 519 (CA). See also Case No 41813 [2002] NZ Priv Cmr 12 (June 2002).

leading to his poor employment outcomes as a teacher, apart from the note on file saying he was a blatant homosexual. These other factors included his reaction to being passed over for promotion, which made him unpopular among his colleagues.[156]

Fourth, there are elements of subjectivity inherent in the text of s 66 of the Privacy Act 2020.[157] Words such as "significant" in the text create uncertainty.[158] Nonetheless, such words play a key role in the availability of remedies, as is seen cases such as *H v Westpac Trust*,[159] and *K v Police Commissioner*.[160] This is an important concern because, according to Associate Professor Stephen Penk, the legal test in s 66 is subjective and the onus is on the plaintiff to prove her case on the balance of probabilities.[161] Tied to this are issues with the evidence of harm. The appearance of the word "may" in the text is not necessarily a sign of hope.[162] This is demonstrated in *C v Countrywide Bank*, where the court required more substantiated evidence about future harm flowing from the privacy breach than mere assertion.[163] Equally, in *Holmes*, the Tribunal found that his claims of emotional harm were exaggerated.[164]

Finally, there are conflicting constitutional imperatives that might muddy the waters in New Zealand. There are similarities among the s 66 harm test, common law invasion of privacy tort and the offensive to a reasonable person test. It is not a mere legislative impulse, but a longstanding common law tradition of "*injuria absque damno*".[165] Certainly the American jurisprudence is based on its common law history and constitutional tradition related to maintaining the separation of powers.[166] Although these parallels in common law history and constitutional imperatives are not binding, it is unlikely they will be wholly ignored.

Section 66 of the Privacy 2020 and similar legal frameworks can be seen as legalisms rooted in their historical context, and possibly serving certain goals. There seems to be jurisprudential disagreement about the application of s 66 and this is vividly illustrated in *Taylor v Orcon*, where the Tribunal overruled the "primary connection" approach to causation taken by the Privacy Commissioner.[167] Even though the Privacy Commissioner later stated that it had learned its lessons, the very fact that the Privacy Commissioner had to be 'corrected' on such a fundamental

156 At 525.
157 See generally Paul Roth (ed) *Privacy Law and Practice* (online looseleaf ed, Lexis Nexis, accessed September 2016) at [PVA66.1]–[PVA66.8].
158 Privacy Act 2020, s 66(1)(b)(iii).
159 *H v Westpac Trust* CRT Decision No 28/99, CRT 15/99, 20 October 1999.
160 *K v Police Commissioner* CRT Decision No 33/99, CRT 17/99, 26 November 1999 at 7.
161 Penk, above n 151, at 61.
162 Privacy Act 1993, s 66(1)(b)(i)–(iii).
163 *C v Countrywide Bank* (1997) 4 HRNZ 100 at 106.
164 *Holmes v Housing New Zealand Corp* [2015] NZHRRT 36 at [35].
165 Daniel Townsend "Who Should Define Injuries for Article III Standing" (2015) 68 Stan L Rev 76 at 79.
166 *Spokeo*, above n 2, at 1547–1548.
167 *Taylor v Orcon* [2015] NZHRRT 15 at [38.1] and [63].

matter hints at jurisprudential disagreement.[168] This highlights the difficulty of applying s 66 ideals consistently. But the debate is not over yet.

C. Systemic Nature of Data Privacy Harms Best addressed at Regulatory Level

It is argued that the systemic nature of the harms posed by data aggregators is best addressed at the regulatory level by legislation separate to the Privacy Act 2020. Therefore, it is imperative to stop treating harms from the data aggregators in the same way as any other privacy harms. It is important to understand why the status quo approach to data aggregators is inadequate. There need to be calls for legislative change that herald this new regulatory approach. The reasons for this standpoint are critical. First, the systemic nature of harm relates to the "novel methodology" of data aggregators.[169] This is different from every day, run of the mill privacy cases that involve some employment or commercial relationship. Even if some aspects of a complaint related to data aggregators can be resolved, there might still be residual systemic concerns. Second, there is little incentive or resource for ordinary people to tackle these systemic concerns. Even assuming adequate knowledge, the time alone taken to bring forward actions would be a barrier for most. Third, data privacy cases involving data aggregators are much more complicated than ordinary cases and intersect with many areas of law. For example, are data aggregators bound to respect collectivist Māori privacy values such as tapu when dealing with genealogical information?[170] Are data aggregators bound to respect the principles of the Treaty of Waitangi?[171] These are questions left unanswered by the Privacy Act and may be worth tackling more squarely in a separate statute related to data aggregators.

A counterargument to this line of reasoning could be: why not conceive of individual cases as prompting systemic changes? The strengths of this line of reasoning are seen in cases such as *Taylor v Orcon*,[172] and *Hammond v Credit Union Baywide*,[173], which generated a lot of publicity involving large sums awarded, and which resulted in training orders being made. Such high-profile cases can address some aspects of systemic concerns, but only to a limited degree. What about matters that were not directly relevant to the case brought before the Tribunal? This leads to

168 Inna Zadorozhnaya "What we learned from Taylor v Orcon" (2 June 2015) Privacy Commissioner <www.privacy.org.nz>.

169 Kate Crawford and Jason Schultz "Big Data and Due Process: Toward a framework to Redress Predictive Privacy Harms" (2014) 55 B C L Rev 93 at 93.

170 Law Commission, above n 17, at 104–106.

171 See *New Zealand Maori Council v Attorney-General* [1987] 1 NZLR 641 (CA) at 661–665.

172 *Taylor v Orcon*, above n 167.

173 *Hammond v Credit Union Baywide* [2015] NZHRRT 6 at [189].

a salient question. How likely is a just outcome for a case that is not high profile? It would also be instructive to consider short-term and long-term cost-effectiveness. Although individual cases may have some impact on systemic concerns in the short-term, in the long-term many more pernicious issues are neglected. The long-term cost of this approach is too much to ignore. It is vital that the law fully addresses systemic harms.

D. A Regulatory Approach Allows for Greater Consistency and a Fairer Balance between Business Interests of Data Aggregators and Human Rights

A regulatory approach to data aggregators, supported by separate legislation on data aggregators, allows for greater consistency. It also allows for a fairer balance between the interests of data aggregators and human rights than does the status quo. It is therefore imperative that the status quo changes by adopting the regulatory approach. Once the regulation is formulated, it can be applied fairly consistently. Even before the law is finalised, the process of introducing a new piece of legislation on data aggregators can engender submissions to a select committee stating the competing views and interests that define the various stakeholders. The notion of balancing is critical to this area of law, and is hinted at under s 14 of the Privacy Act.[174] In *Balfour*, the Court of Appeal noted the social good that is served by the education file, notwithstanding the risks posed by inaccurate notes on these files.[175] Equally, if data aggregation is carried out in a properly regulated fashion it could result in some social good. It seems clear that the legal status quo does not ensure a proper balance between competing interests. Rather, separate legislation can and must specifically detail how this balance is going to be achieved. Such an approach will avoid confusion and reduce the complexity of dealing with data aggregators according to the existing framework.

E. A Blanket Policy of Loosening the Harm Requirement will not Work

It is argued that merely loosening the harm requirement in the Privacy Act will not lead to optimal outcomes and may encourage or fail to prevent vexatious litigation. Therefore, the argument goes that the Privacy Act's harm requirement should remain unchanged for ordinary data privacy cases. However, a different set of legislation is needed to herald the new regulatory approach, which removes

174 Privacy Act 1993, s 14.
175 *Balfour*, above n 155, at 528.

the harm requirement for cases involving data aggregators due to the nature of their harms. Loosening the harm requirement is likely to prompt 'floodgates' concerns, not only for cases involving data aggregators but also for a wide gamut of privacy cases that do not involve the special circumstances related to privacy harms by data aggregators.[176] This is a risk because disputes before the Privacy Commissioner and Human Rights Review Tribunal (HRRT) may go beyond privacy concerns to encompass other matters. There is a risk that, if defeated in one area, the litigant may attempt to litigate via the privacy route.[177] Some complainants try to use the complaints process to dignify so-called "empty your pockets" requests for information which can incur a considerable cost at times.[178] However, these challenges are not insurmountable and can be dealt within the regulatory response.

V. Proposed Model of Regulation of Data Aggregators

This article proposes the following model of enforcement and regulation of data aggregators.

The model of enforcement of data aggregators will consist of a *sui generis* piece of legislation that specifically centralises the issues posed by data aggregators in respect of data privacy law. A key aspect of this legislation which will encompass the model of regulation is that it will set up a code of conduct for data aggregators. This could include aspects such as transparency, including algorithmic transparency, and include a similar statement to that of the GDPR on automated processing and the role of permission in terms of actions by data aggregators.[179] In fact, the code of conduct should mirror some of the relevant articles of the GDPR, including arts 13, 21 and 22. The model should also address the interrelationship between public registers and data aggregators, including the role of permission when collecting information from public registers, clarifying illegal activities and the right to erasure and destruction of stale data. It should cover the use of data aggregators by third parties, including government departments. This links with the issue of automated processing outlined in art 22 of the GDPR. The issue of market power and dominance needs to be addressed. This entails addressing competition law issues. The central question is whether data aggregators hold too much power in the market with respect to objects of competition law.

176 See generally *Alcock v Chief Constable of South Yorkshire* [1991] UKHL 5.

177 Gehan Gunasekera 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 at 245.

178 *O'Neil v Dispute Resolution Services Ltd* [2006] NZHRRT 15 at [86].

179 Office of the Privacy Commissioner, above n 22, at [1.9 (d)].

According to Eric Everson "... at present, the most popular Big Data tools do not include strong, automated safeguards related to post-contextual analysis of output data".[180] This means the technology is only being used one way, to exploit consumer data, but the potential harms are not analysed within the algorithm. The proposed model will ensure that data aggregators that are able to operate legally are licenced in the same way doctors and lawyers are licenced and that the Privacy Commissioner is able to participate in this licencing process alongside a panel of experts.[181] The reason for a separate model of regulation is due to the nature of privacy issues of data aggregators.

One crucial theoretical aspect of this proposed model of enforcement is that it will tailor the concepts underlying Privacy by Design (PbD) to data aggregators, in particular, foundational principles of PbD such as a culture of continuous improvement, privacy embedded in design and the motto "proactive not reactive, preventative not remedial".[182] By adopting PbD into the building blocks of the model, the model can respond effectively to Varuhas and Moreham's commentary about the reactive nature of privacy law remedies.

Ann Cavoukian sums up the theory of PbD:[183]

> The Privacy by Design Approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Several commentators and policy think tanks now canvass the concept of PbD, most notably several submissions to the Bill of the recently passed Privacy Act 2020 called upon the Select Committee to give effect to PbD in the Bill.[184] PbD is also incorporated into art 25 of the European Union`s GDPR.[185] Ann Cavoukian also suggests some structural supports to give effect to the goals of PbD including "... established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, correct any negative impacts, well before they occur in

180 Eric Everson "Privacy by Design: Taking Control of Big Data" [2016] 65 Clev St L Rev 27 at 31.
181 See Law Commission, above n 46, at 86.
182 Ann Cavoukian "Privacy by Design; The 7 Foundational Principles; Implementation and Mapping of Fair Information Practices" The International Association of Privacy Professionals (IAPP) <www.iapp.org> at 3.
183 At 2.
184 See Catalyst "Submission to the Justice and Electoral Committee on the Privacy Bill" at [3.2].
185 GDPR, art 25.

proactive, systematic, and innovative ways".[186] The proactive nature of this model is a key feature, which distinguishes it from the status quo. The status quo is reactive. There is no specific legal mechanism to deal with data aggregators in the status quo. The issue falls within the general ambit of the Privacy Act, which arguably has been weakened since the last reform. The proposed model consists of a piece of legislation that will outline some of the harms posed by data aggregators and will address them in turn. The model for regulation should allow for the diverse nature of data aggregators. It is not meant to be perfect, but it is a start.

A further aspect is the new pool of funding provided to the Privacy Commissioner and HRRT to deal with these specialised cases. This will entail HRRT hiring another commissioner.[187] Equally, the Privacy Commissioner will have a further function of educating the public about data aggregators by holding information events which attempt to reduce the informational asymmetry between the public and data aggregators.

In terms of remedies, there should be a streamlined process of complaints for data aggregators, a separate branch set up within the Privacy Commissioner to deal with data aggregator cases, giving greater access to HRRT and taking away unnecessary barriers, allowing collective complaints by organisations on behalf of individuals and removing the harm requirement for cases involving data aggregators.

The victims of prospective privacy harms of data aggregators should not be subject to limits posed by s 66 of the Privacy Act 2020. The proposed model will ensure that victims of data aggregator will get a prima facie remedy if an interference with privacy is established, without having to establish harm. It is argued that the floodgates issues associated with the normal privacy regime will not apply to cases involving data aggregators. The Law Commission has canvassed this earlier and it states:[188]

> We were told that the harm threshold works imperfectly in filtering out less deserving cases. Removing the harm requirement would be easier for complainants to understand, would allow more consistent enforcement, and, in particular, could be useful in exposing systemic problems which have the potential to cause harm if left unattended to.

186 Cavoukian, above n 182, at 2.

187 New Zealand Law Society "Submission to the Justice and Electoral Committee on the Privacy Bill" at [68] and [70].

188 Law Commission Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 (NZLC R123, 2011) at 179.

Equally, the additional funding will be used to deal with any increased workload of cases. There should also be a change to award exemplary damages for cases involving data aggregators. This will represent a shift from the status quo, where exemplary damages are augmented by the wording of s 57(1)(d) of the Health and Disability Commissioner Act 1994, which grants the HRRT the power to award damages for "any action of the defendant that was in flagrant disregard of the rights of the aggrieved person".[189] In fact, the proposed legislation will go much further than the Health and Disability Commissioner Act 1994; since it will actually clarify that the purpose of damages is for punishment and that they are not purely compensatory as outlined in the privacy jurisprudence under the status quo. It is argued that data aggregators should be held to the higher standard than any other data agency because of their immense power and the nature of their harms.

VI. Conclusion

This article argues that that the current path for justice for victims of data privacy harms from data aggregators is akin to walking a tightrope. Consequently, the model put forward in this article aims to make the journey to justice more akin to a walk on a bridge. These reasons are both legal and policy-oriented.

Instead of trying to fit data aggregation issues in an ad-hoc manner into a privacy framework that does not accommodate them, it is time to have a public conversation on the risks posed to individual rights by data aggregators. This should culminate in the passing of a law that addresses the broad range of prospective harms that stem from data aggregators. Before such a bill is passed, submissions from various stakeholders would be sought. This will allow for a clear consensus on where the public and other groups believe the balance should be struck. It might allow for some legitimate business imperatives of data aggregators.

The regulatory route better addresses the knowledge gap that acts as a barrier to effectively addressing inaccurate data profiles. These inaccuracies are likely to be symptomatic of inadequate or non-compliant internal procedures amongst data aggregators. Regulation can be a safety net to protect against the dual effects of lack of knowledge by victims and superior knowledge and resources on the part of data aggregators, which delay or prevent complaint cases, creating a vicious cycle. Although unprincipled regulatory approaches pose risks to optimal outcomes, clear checks can make them more proactive. It is predicted that if a case similar to *Spokeo* were to arise in New Zealand, it would be difficult for the plaintiff to meet the harm requirement. Therefore, there should be targeted regulation of data

189 Health and Disability Commissioner Act 1994, s 57(1)(d).

aggregators separate from the Privacy Act. This would provide a counter to the way the Act is interpreted against its legislative history, purpose and the wider common law background, all of which display caution in taking an expansive approach to harm. There may be good reason for this, because the Act is designed to deal with all types of privacy issues, and was enacted prior to the explosion of data aggregation. Unsurprisingly, therefore, the current framework is subject to loopholes that data aggregators can exploit, relying on extensive funds to meet legal costs.

In an era of vast technological change and the advent of "surveillance capitalism", New Zealand's data privacy law cannot afford to lag behind. It has to fully address data harms by data aggregators through a specific layer of regulation. Although this would not render the New Zealand privacy complaints system obsolete, it can better encompass the conceptual complexity of issues posed by data aggregators. In light of New Zealand's individually oriented complaints system, it is important to see whether it can properly address a case similar to *Spokeo.* It is argued that in the era post-*Taylor v Orcon* and subsequent HRRT cases including *Dotcom*, there is a greater likelihood that a complainant in a similar situation to Mr Robins would not get recourse.

The crux of the matter is that the New Zealand Privacy Act is a product of its time. It was formulated the early 1990s, the era of the bulky computer. Since then, both technology and the legal issues attached to privacy have well outpaced the capability of existing law to deal effectively with them. The harm requirement in s 66 of the Privacy Act is a key part of this phenomenon. The harm requirement is impacted by s 14 of the Privacy Act, which requires the Privacy Commissioner to balance business interests with privacy rights. However, the Privacy Act was enacted at a time when the risks posed by data aggregators were not apparent. Further, the Privacy Act sets up a system of complaints that deal with a wide gamut of privacy issues, not just those about the data aggregators. This means that reforming the Privacy Act may have collateral impacts on other legal cases. The premise is that there is no pure privacy case. So the risk is that if a complaint fails in another area of law, the complainant uses the privacy law route to litigate their case further. The particular causation rules are based on the common law tradition, and they do not need to change. A key aspect of the case for the regulatory approach is that data aggregators' operations involve systemic privacy issues. These issues, as the Law Commission emphasises, cannot be fixed solely by individual complaints.

A *sui generis* legislative scheme, specifically focusing on data aggregators and their prospective privacy harms, is imperative. Otherwise, New Zealand is putting citizens' privacy rights at serious risk. These include the right to informational self-determination and more specific rights that exist within the statutory

framework. This is because New Zealand's current privacy framework did not have data aggregators at the forefront when the law was formed. The knowledge gap and the power imbalance between data aggregators and those whose data is being collected are vast. Data aggregators use sophisticated technology and tactics that can leave the savviest members of the public by the wayside when it comes to their privacy rights. If the system based on the New Zealand Privacy Act alone continues, it will aggravate unfairness for those who suffer from the rogue practices of data aggregators.