ON THE (DATA) BREACH OF CONFIDENCE

MATT MALONE*

I. INTRODUCTION

In the last decade, the evolution of the breach of confidence as a legal instrument to redress harms occurring in digital realms has tested the limits of this cause of action and raised significant questions about the legal interests it serves to protect.[1] A hybrid action whose foundations do not "rest solely on one of the traditional jurisdictional bases for action of contract, equity or property," the traditional *mise en scène* of the breach of confidence has been the employment setting.[2] The scenarios giving rise to its use have centred on departing employees misappropriating trade secrets or confidential information.[3]

That traditional setting, though, has not halted efforts by parties to deploy the breach of confidence to sanction, protect, and instantiate norms of trust in novel relationships formed outside of the employment context, in particular in relationships that form and occur online. Such attempts to extend the breach of confidence have received uneven endorsement from Canadian judges. For example, in disputes involving the unauthorized distribution of intimate images of an individual without the individual's permission (where the unauthorized distribution of those images occurs in betrayal of relationships of trust in which they were originally taken and shared), judges have been generally receptive to the use of the breach of confidence.[4] This trend has received ample commentary in recent years.[5]

This case comment focuses on another type of dispute — one where courts have been far more equivocal in their approach — where parties have sought to assert the breach of confidence for wrongs occurring in online relationships: data breaches. Focusing on *Tucci v. Peoples Trust Company*, this comment scrutinizes the reading of the breach of confidence that Canadian courts have been making in the context of data breaches, and contends that this reading ignores the essence and promise of this cause of action to instill trust in online relationships that are threatened when data breaches occur.[6] The judgment in *Tucci* was handed down by the Court of Appeal for British Columbia in September 2020 on appeal of

---

* PhD Candidate, Faculty of Law, University of Ottawa.

1 See generally Gavin Phillipson, "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act" (2003) 66:5 Mod L Rev 726; Jonathan Morgan, "Privacy, Confidence and Horizontal Effect: 'Hello' Trouble" (2003) 62:2 Cambridge LJ 444; Jillian Caldwell, "Protecting Privacy Post *Lenah*: Should the Courts Establish a New Tort or Develop Breach of Confidence?" (2003) 26:1 UNSWLJ 90; Chris DL Hunt, "From Right to Wrong: Grounding a 'Right' to Privacy in the 'Wrongs' of Tort" (2015) 52:3 Alta L Rev 635.

2 *Lac Minerals Ltd v International Corona Resources Ltd*, [1989] 2 SCR 574 at 615 [*Lac Minerals*].

3 See Mark A Lemley, "The Surprising Virtues of Treating Trade Secrets as IP Rights" (2008) 61:2 Stan L Rev 311.

4 See *Doucet v The Royal Winnipeg Ballet*, 2018 ONSC 4008. See also *Doe 464533 v ND*, 2016 ONSC 541.

5 See generally Hannah EY Choo, "Why We Are Still Searching for Solutions to Cyberbullying: An Analysis of the North American Responses to Cyberbullying Under the Theory of Systemic Desensitization" (2015) 66 UNBLJ 52; Siobhan O'Brien & Marie-Évelyne Danik, "New Privacy Tort: Public Disclosure of Private Embarrassing Facts" (Paper delivered at the 36th Annual Civil Litigation Conference, 18–19 November 2016), 2016 CanLIIDocs 4382; Suzie Dunn & Alessia Petricone-Westwood, "More than 'Revenge Porn' Civil Remedies for the Non-Consensual Distribution of Intimate Images" (Paper delivered at the 38th Annual Civil Litigation Conference, 16–17 November 2018), 2018 CanLIIDocs 10789.

6 2020 BCCA 246 [*Tucci* CA].

a decision certifying a class of web users whose personal information was subject to unauthorized acquisition in a data breach. Contrary to judicial reluctance to allow the breach of confidence to operate in these scenarios, this comment argues that this cause of action is an appropriate and effective mechanism for establishing and reinforcing norms of trust in online relationships that are threatened when data breaches occur. It advocates expanding the meaning of unauthorized use and using the breach of confidence to recognize the responsibilities of effective stewardship and protection of data incumbent on data guardians who hold themselves out as capable of safeguarding and securing data and assigning them liability when they fail to do so in a data breach.

II. THE PROBLEM OF UNAUTHORIZED USE

At the outset, two definitions and an observation of the problem.

A data breach is the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector."[7] During a data breach, the personal information of an individual that has been placed in the hands of a guardian of that data is accessed by a third party without the consent of the individual. Although in most data breach cases, "there is evidence that the defendants failed to use reasonable care in securing plaintiffs' data," the nature of and reason for data breaches varies.[8] On the one hand, they may occur due to a failure to take precautions and conduct proper monitoring. On the other hand, they may occur even where such precautions were taken but unauthorized acquisition occurred due to a sophisticated attack launched by nation-states, hackers, terrorist groups, thrill-seekers, or rogue employees operating inside a network.[9] Data breaches have been growing in frequency and scale in recent years.[10]

The breach of confidence is a cause of action offering legal protection for the misappropriation of information imparted in confidence that is subject to unauthorized use. This cause of action "rest[s] on judge made law," and "pre-suppose[s] a course of conduct or dealings between a plaintiff and a defendant prior to the misappropriation."[11] In Canada, the breach of confidence enunciated in *Lac Minerals* enshrined this cause of action as it was crystalized in the English case *Coco v. AN Clark (Engineers) Ltd.*[12] The elements of the breach of confidence are: (1) the information must have the necessary quality of confidence about it; (2) the information must have been imparted in circumstances importing an obligation of confidence; and (3) there must have been an unauthorized use of that information to the detriment of the party communicating it.[13]

---

7 International Association of Privacy Professionals, "Data Breach," online: <iapp.org/resources/article/data-breach/>.

8 Daniel J Solove & Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (2018) 96:4 Tex L Rev 737 at 739.

9 Alison DeNisco Rayome, "12 Reasons Why Data Breaches Still Happen," online: <www.techrepublic.com/article/12-reasons-why-data-breaches-still-happen/#:~:text=It%20is%20difficult%20to%20protect,a%20phishing%20scam%20(61%25)>.

10 See generally Sasha Romanosky, David Hoffman & Alessandro Acquisti, "Empirical Analysis of Data Breach Litigation" (2014) 11:1 J Empirical Leg Stud 74.

11 Institute of Law Research and Reform, *Trade Secrets*, Report 46 (Edmonton, 1986) at 17, online: <www.alri.ualberta.ca/1986/07/trade-secrets/>.

12 [1969] RPC 41 (Ch D) (UK) [*Coco*].

13 *Lac Minerals*, *supra* note 2 at 608.

In applying the breach of confidence to a data breach, courts resorting to the *Coco* test encounter an important hurdle. Although judges may find that the data provided by an individual to a data guardian possesses the necessary quality of confidence and that the transmission occurred in circumstances generating obligations of confidence, courts have struggled with the third prong of the test — the unauthorized use of the information. Trouble arises from the fact that the data guardian does not appear to effect unauthorized use, such as using the data for a purpose for which there was no consent. Rather, the party appearing to effect unauthorized use is the one who commits the unauthorized acquisition of the data. In light of this salient fact, judges are often wont to locate fault on the part of the data guardian for any action they may (or may not) have taken.

III. *TUCCI V. PEOPLES TRUST COMPANY*

The recent case of *Tucci* is a textbook example of a data breach.[14] In or about September 2013, cybercriminals located in the People's Republic of China gained access to the databases of Peoples Trust Company (Peoples Trust), a federally regulated trust company. The databases contained the unencrypted personal information of Peoples Trust's website users collected through its web portal (including their "name, address, telephone number, email address, date of birth, Social Insurance Number, and occupation").[15] The cybercriminals then sent unsolicited text messages to the users asking them to call a phone number in Utah for the purposes of phishing.[16] All told, the personal information of approximately 11,000–13,000 customers was accessed during the data breach.[17]

Following a forensic investigation by the defendant, Peoples Trust notified the RCMP and also underwent an investigation by the Privacy Commissioner of Canada, which found that Peoples Trust "did not implement sufficiently strong safeguards in developing its online application web portal in order to protect the sensitive personal information being collected from customers."[18] In the report of its investigation, the Privacy Commissioner also criticized the lack of a security policy and a lack of ongoing monitoring by Peoples Trust, and criticized the fact that an unencrypted copy of the data had been left "on a web server that had not been updated to address a well-known vulnerability."[19] At the same time, the Privacy Commissioner recognized that the company implemented responsive measures in a timely manner after the data breach occurred.[20]

On 25 October 2013, Peoples Trust notified approximately 11,000–13,000 individuals about the breach.[21] One of those individuals, Mr. Tucci, a resident of Windsor, Ontario, initiated a class proceeding as a representative plaintiff against Peoples Trust, for failure to safeguard his and other putative class members' personal information accessed during the

---

14 *Tucci v Peoples Trust Company*, 2017 BCSC 1525 [*Tucci* SC]. See also *Tucci* CA, *supra* note 6.
15 *Tucci* SC, *ibid* at para 10.
16 *Ibid* at para 15.
17 *Ibid* at para 18.
18 *Ibid* at para 23, citing Office of the Privacy Commissioner of Canada, *Privacy Protection: A Global Affair, Report on the* Personal Information Protection and Electronic Documents Act, Catalogue No IP51-1E-PDF (Gatineau: Office of the Privacy Commissioner of Canada, 2015) at 19, online: <www.priv.gc.ca/media/1701/2014_pipeda_e.pdf>.
19 *Tucci* SC, *ibid*.
20 *Ibid*.
21 *Ibid* at para 18.

breach.[22] Perhaps as a sign of the lack of clarity that surrounds the proper legal recourse for plaintiffs to pursue in a data breach proceeding, Tucci brought an array of claims against Peoples Trust, pleading breach of contract, negligence, breach of privacy, and intrusion upon seclusion, and, in the alternative, unjust enrichment. He also brought a claim, *inter alia*, for the breach of confidence.[23]

At first instance, the trial judge tacitly accepted the plaintiff's pleadings that the information in question was confidential in nature and that it had been imparted in confidence, fulfilling the first two prongs of the test for the breach of confidence outlined in *Coco* and recognized in *Lac Minerals*.[24] However, focusing on the final prong of the test in *Coco*, the trial judge hesitated to articulate the harm caused by the data breach as an instance of unauthorized use. "[I]t is clear," the trial judge wrote, "that in order for there to be misuse, there must be use for a non-permitted purpose. The plaintiff has not pleaded any facts capable of establishing that the information was used for a non-permitted purpose.… As the misuse element has not been properly pleaded, this cause of action must fail."[25] Notably, the trial judge also acknowledged Peoples Trust's multiple technical failures to safeguard the data, which suggests that the failure to protect data kept for business purposes would never present facts capable of establishing use for a non-permitted purpose. This is especially true given Peoples Trust's failure to encrypt the data — perhaps the most basic, simple, and obvious safeguard it could have taken. Thus, although the trial judge left a possible opening here, one is left to wonder what use for what non-permitted purpose would satisfy the requirement of establishing unauthorized use. The trial judge proceeded to certify the action as a class proceeding only on the claims of breach of contract and negligence.

On appeal, the Court of Appeal gave a cursory affirmation of the trial court's dismissal of the breach of confidence claim. Referring to the breach of confidence as "well-defined as an intentional tort,"[26] Justice Groberman noted the trial judge's finding of an absence of unauthorized use.[27] Although Justice Groberman acknowledged two other class proceedings where the breach of confidence was accepted at the pleading stage (albeit with no discussion of the merits),[28] his most striking comment was that "[o]ther torts, such as negligence and (assuming they exist) breach of privacy and intrusion upon seclusion are more appropriate vehicles to deal with inadvertent disclosure of data."[29]

The need for a prerequisite finding of unauthorized use would seem to pose an insurmountable challenge for parties arguing the breach of confidence in a data breach case, both in class certification proceedings as well as on the merits. As respected class actions jurist Justice Edward P. Belobaba wrote in a data breach case in Ontario: "[u]nless the word

---

22 *Ibid* at paras 2, 7.
23 *Ibid* at para 2.
24 *Ibid* at paras 137, 140.
25 *Ibid* at paras 141–43.
26 *Tucci* CA, *supra* note 6 at para 113. The breach of confidence is often referred to as a *sui generis* action that has legal and equitable elements. See *Cadbury Schweppes Inc v FBI Foods Ltd*, [1999] 1 SCR 142 at para 26 [emphasis in original]: "whether a breach of confidence in a particular case has a contractual, tortious, proprietary or trust flavour goes to the *appropriateness* of a particular equitable remedy" and at para 49: "[t]he House of Lords has subsequently affirmed that actions for breach of confidence are equitable in nature."
27 *Tucci* CA, *ibid* at para 111.
28 See *John Doe v Canada*, 2015 FC 916; *Condon v Canada*, 2015 FCA 159.
29 *Tucci* CA, *supra* note 6 at para 113.

'misuse' is distorted out of all shape and meaning, the defendants' failure to prevent the cyber-attack is not a 'misuse' of confidential information within the meaning of the breach of confidence tort."[30] Of course, the literalist reading of unauthorized use has proven less challenging in cases involving the disclosure of sensitive images that were imparted in confidence. In such disputes, the act constituting unauthorized use is highly conspicuous: it occurs with the disclosure of the images. For this reason, judges have been far more welcoming of the breach of confidence in those cases.[31] In a rare instance of codification, the breach of confidence has even been incorporated into the definition of "cyber-bullying" in Nova Scotia's *Intimate Images and Cyber-protection Act*.[32]

The injustice here is that the motive of a data breach is undoubtedly misuse, albeit by the party making an unauthorized acquisition of the data. In *Tucci*, the trial and appellate justices, like Justice Belobaba, both posited that the actions (or non-actions) of Peoples Trust could not constitute unauthorized use in any literal sense. The trial judge appeared to resist oversimplification, noting that the breach of confidence is not so narrow as to restrict misuse to "obtain[ing] a profit" and thus leaving open the possibility of a finding of misuse where the pleading elucidated "facts capable of establishing that the information was used for a non-permitted purpose."[33] However, the trial judge elsewhere acknowledged the multiple technical failures of Peoples Trust, including the failures to have a comprehensive security policy, to monitor on a continuous basis, and to use encryption.[34] Based on this comprehensive list, the trial judge's holding implicitly acknowledged that storing and using data for business purposes *without* taking adequate precautions would not rise to a finding of "use for a non-permitted purpose."[35]

Such a holding is lamentable, as it ignores the reality that unauthorized use may have occurred in the actions of Peoples Trust by their failure to protect and safeguard the data in the first place. Such failures included not taking adequate precautionary measures, such as encrypting data as the federal government's Canadian Centre for Cyber Security (CCCS) recommends,[36] as well as not having in place an action plan in the event of a data breach, another CCCS recommendation.[37] These oversights were all the more significant given that the name of the company itself embedded "trust" in the relationship with users.[38] Rather than finding liability under the breach of confidence for Peoples Trust's failure to adequately safeguard data it possessed, the trial and appellate Courts absolved Peoples Trust of liability for actions it did not take to prevent misuse of that data. Under such a reading, of course,

---

30 *Kaplan v Casino Rama*, 2019 ONSC 2025 at para 31.

31 See *supra* note 4.

32 SNS 2017, c 7, s 3(c)(iii).

33 *Tucci* SC, *supra* note 14 at para 141.

34 *Ibid* at para 110.

35 *Ibid*.

36 Canadian Centre for Cyber Security, *Baseline Cyber Security Controls for Small and Medium Organizations v 1.2* (Ottawa: Communications Security Establishment, 2020) at s 3.7, online: <cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>.

37 *Ibid*, s 3.1.

38 At the same time, it is worth recalling what did not occur in *Tucci*. As noted above, there is no single type of data breach. In *Tucci*, the breach did not occur because a rogue employee with access to data as part of their job subsequently copied these data and shared them with an unauthorized user. In such an event, Peoples Trust likely would have been found not vicariously liable; thus, liability under the breach of confidence could not attach to the employer to the data breach. This was situation in the recent factual scenario and ruling of the Supreme Court of the United Kingdom decision *WM Morrison Supermarkets plc v Various Claimants,* [2020] UKSC 12.

even if Peoples Trust had taken no measures to safeguard the data, liability could not attach under the breach of confidence, so long as there was no proactive misuse. Yet this runs counter to the expectations of individuals who provide confidential information in a confidential manner to financial institutions, which hold themselves out as secure and trustworthy guardians of that data. The principles of trust seem to suggest that those individuals have a right to expect that their data is secure. Since 2019, federally regulated financial institutions are held to a broader standard of what constitutes technology and cyber security incidents by the Office of the Superintendent of Financial Institutions Canada.[39]

The problem with removing the breach of confidence in these scenarios is the lack of alternative recourse. For example, the *Personal Information Protection and Electronic Documents Act* hardly provides effective recourse to a putative class in data breach scenarios, since damages are not generally available through the *Act*.[40] The proposed *Consumer Privacy Protection Act* (Part 1 of Bill C-11 of the 43rd Parliament) makes available damages for injury engendered by a contravention of the *Act*.[41] However, contraventions related to data breaches only concern failing to provide notice to consumers of a "breach of security safeguards … that involves personal information."[42] In other words, the provisions set forth in Bill C-11 still fail to enhance the onus on organizations to take adequate security measures.

Instead, defendants must turn to civil law, in particular contract and negligence, greatly limiting the means of redress available. It was here that the representative plaintiff in *Tucci* succeeded. The trial and appellate Courts upheld the breach of contract claim in light of the obligations that Peoples Trust set forth in its "Website Terms & Conditions."[43] (At the same time, the Court left the limitation of liability clause for trial, suggesting that a breach of contract claim may not even succeed on the merits.)[44] Further, the basis for a negligence claim was largely found in duties that were "said to arise from the organization's own privacy policies" (as opposed to objective duties, leaving them open to contractual limitation in the future).[45] However, the appellate Court did note that a data breach could "create a relationship giving rise to a duty of care" (that is, separate from contract), but did not provide any guidance on whether technical failures by a data guardian would trigger the existence of such a duty.[46]

The holding in *Tucci* stands for a view that data guardians may continue to set the standards to which they will be held accountable — no doubt an important strategic takeaway from the case for data guardians. The reading of the trial and appellate Courts in

---

39 Office of the Superintendent of Financial Institutions Canada, *Advisory: Technology and Cyber Security Incident Reporting*, (2019), online: <osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx>.

40 SC 2000, c 5, s 16(c) [*PIPEDA*]. A complainant bringing a complaint to the Privacy Commissioner, after receiving the Privacy Commissioner's report, may be awarded damages by a court. However, this remedy does not provide collective relief in the event of a data breach.

41 Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020, cl 106 (first reading 17 November 2020).

42 *Ibid*, cl 61.

43 *Tucci* SC, *supra* note 14 at paras 110–12; *Tucci* CA, *supra* note 6 at paras 41–49.

44 *Tucci* SC, *ibid* at para 112.

45 *Ibid* at para 131.

46 *Tucci* CA, *supra* note 6 at para 51.

Tucci suggests that the representative plaintiff and putative class members assumed the risk in their information being inadvertently disclosed when they shared it with Peoples Trust. This reading contrasts with one where Peoples Trust assumed responsibility by failing to meet appropriate standards of safeguarding data beyond the terms of set forth by contract. If the Courts had privileged a reading where "the focus of the tort of breach of confidentiality [was] on the nature of the relationship," rather than the fate of the information, certain facts in the case would have assumed different importance — in particular the failures of Peoples Trust to safeguard the data.[47] The significance of the Courts' decision to reject the breach of confidence cause of action jettisons a powerful way in which the courts could otherwise enforce and uphold the responsibilities incumbent on data guardians in protecting individuals' data.

IV. PRIVACY DISCOURSE AND THE BREACH OF CONFIDENCE

On a broader level, the reluctance of the trial and appellate Courts to utilize the breach of confidence in this situation is attributable to two key reasons. The first is the judiciary's patience to see what fruits bear from the proliferation of new privacy torts that are emerging in common law jurisdictions, such as the tort of the invasion of personal privacy, or intrusion upon seclusion, developed by the Court of Appeal for Ontario in *Jones v. Tsige*.[48] The Court of Appeal for British Columbia itself noted in *Tucci* that it views these torts as appropriate vehicles for remediation.[49] The tort of public disclosure of private facts has also made headwinds in Ontario.[50] The House of Lords, too, has acknowledged that the shortcomings of the breach of confidence may need to be repaired by using an explicit privacy tort.[51] Although such a tort was argued at first instance in *Tucci*, it was removed by the trial judge, and thus, not recognized by the Court of Appeal. Nevertheless, the *obiter dicta* in the appellate decision invites provincial and federal counterparts to continue to recognize such torts.[52]

Secondly, judicial reluctance to recognize failure to take adequate measures to safeguard data as unauthorized use is indicative of a particular privacy discourse coursing throughout the holding. This discourse privileges the rights of an individual's inviolate privacy over the nature of the relationship at hand. Neil Richards and Daniel Solove have noted how the development of privacy in the United States grew around "protecting the information we hide away in secrecy" rather than "our expectations of trust and reliance in relationships."[53] To recall, the breach of confidence was developed in the interest of enforcing business morality and commercial ethics in relationships.[54] The emphasis fell not strictly on the information that transacted between parties, but rather the relationships of confidence in which it was

---

47 Neil M Richards & Daniel J Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96:1 Geo LJ 123 at 174.

48 2012 ONCA 32.

49 *Tucci* CA, *supra* note 6 at para 113.

50 See *Jane Doe 72511 v NM*, 2018 ONSC 6607.

51 *Campbell v MGN Limited*, [2004] UKHL 22 at para 14: "[i]nformation about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information."

52 *Tucci* CA, *supra* note 6 at para 113.

53 Richards & Solove, *supra* note 47 at 125.

54 See generally "Object of the Protection" in Elizabeth F Judge & Daniel J Gervais, *Intellectual Property: The Law in Canada*, 2nd ed (Toronto: Carswell, 2011) at 889–902.

transacted. This emphasis has been dislocated by a shift towards privacy, whose definitional feature involves placing the emphasis on inviolate individual personality rights rather than social relationships.[55] The key difference between privacy torts and the breach of confidence "is the nature of what is protected. The public disclosure tort focuses on the nature of the information being made public. By contrast, the focus of the tort of breach of confidentiality is on the nature of the relationship."[56] To this point, Richards and Solove refer to the copious torts surrounding the right of privacy that have emerged in the United States, in contrast to Britain's reluctance to develop such law.[57]

One of the key problems with this conceptualization is that it manages privacy rights through a consent model premised on contract. This privacy self-management model, although dominate in judicial thinking about privacy, has been the subject of deep criticism for the way it conceptualizes privacy as "a series of isolated transactions guided by particular individuals."[58] The reasons for criticism of this model are many, but, as a crucial starting point, empirical studies repeatedly show that nobody reads privacy notices.[59] This is almost certainly true of the representative plaintiff and putative members of the class in *Tucci* when they clicked through the "Website Terms & Conditions." Beyond the fact that people do not read privacy notices, other cognitive problems have been the subject of critique of the privacy self-management model, including the fact that even when individuals read privacy agreements, they do not understand them.[60] Individuals often lack sufficient background to make informed choices about privacy agreements, and choice itself is affected by heuristics in the manner in which such agreements are presented to users.[61]

Moreover, this privacy self-management model is ill-equipped to respond to collectivized harms wrought by data breaches. As Teresa Scassa notes: "[i]ndividual-oriented consent-based mechanisms no longer seem adequate or appropriate to address the challenges posed by the ubiquitous and continuous harvesting of massive amounts of data."[62] Just as class action proceedings were developed to fill the procedural void that prevented the legal system from providing redress for harms visited on individuals, as discrete occurrences, so too are the harms experienced by data breaches more than simply individual wrongs that should be redressed by breach of contract and negligence. (To be clear, data breaches in the public sector — such as the one in 2020 of Revenue Canada's website that resulted in the unauthorized acquisition of 5,500 users' data[63] — are susceptible to public law protections such as sections 7 and 8 of the *Canadian Charter of Rights and Freedoms*,[64] though further research and case law will determine if this presumption comes true.) As Scassa notes, the

---

55 Richards & Solove, *supra* note 47 at 133.
56 *Ibid* at 174.
57 *Ibid* at 126.
58 Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126:7 Harv L Rev 1880 at 1881.
59 *Ibid* at 1884.
60 *Ibid* at 1888.
61 *Ibid*.
62 Teresa Scassa, "A Human Rights-Based Approach to Data Protection in Canada" in Elizabeth Dubois & Florian Martin-Bariteau, eds, *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa: University of Ottawa Press, 2020) 173 at 173.
63 Raisa Patel & Philip Ling, "CRA Shuts Down Online Services After Thousands of Accounts Breached in Cyberattacks," *CBC News* (15 August 2020), online: <www.cbc.ca/news/politics/canada-revenue-agency-cra-cyberattack-1.5688163>.
64 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Cambridge Analytica scandal of 2017 demonstrated that although the harms resulted from the misuse of individuals' information, "the most important harms were public ones: the manipulation of voters with a view to subverting democracy."[65]

These observations suggest that responsibility for collectivized harm necessitates solutions that go beyond the individually oriented models of consent that are limited by contract. The collective and society level problems that arise from data breaches suggest the need for new norms to be established and affirmed.[66] Although the breach of confidence presented an opportunity to shift the focus away from contract's "individual-oriented consent-based mechanism" to the norms in the relationship articulated through the breach of confidence, in particular in cases where precautions would have prevented the data breach in the first place, the courts have been declining to do so.[67]

V. TOWARDS A DATA BREACH OF CONFIDENCE?

As an existing device, the breach of confidence may be an excellent tool to enforce norms that the privacy self-management model, by its nature, has failed to enforce. Many of these norms are already understood to exist in relationships that occur in digital spaces, although the legal framework has struggled to respond to them. For example, *PIPEDA*'s framework does an effective job of requiring notification about breaches,[68] with penalties for failing to do so (though these fines are nominal.)[69] The introduction of Bill C-11 on 17 November 2020 makes available a private right of action for individuals suffering harm engendered by a contravention of provisions in the Bill, with a statute of limitations of two years and an unlimited cap on damages.[70] However, the contraventions pertinent to data breaches are merely failure to give notice — and the Bill is currently languishing in parliamentary review. Thus, although a statutory response may present an alternative to extending the breach of confidence, the problem with any statute will be the need to continue to revise it — a peril for statutes concerning something as novel and evolutive as data breaches. Meanwhile, the breach of confidence could serve as a sustainable model, given its proven durability over the last two centuries and its demonstrated flexibility in providing judges with power to craft suitable remedies.

Extending the breach of confidence in this way could also achieve many of the goals sought by Jack Balkin's proposal of the information fiduciary, "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."[71] The information fiduciary model proposed by Balkin was designed to create responsibility for commercial actors handling individuals' data in the same way that the common law already assigns such responsibility to certain professionals such as lawyers, doctors, and accountants. Such professionals, he

---

65 Scassa, *supra* note 62 at 176.
66 See Titus Stahl, "Indiscriminate Mass Surveillance and the Public Sphere" (2016) 18:1 Ethics & Information Technology 33.
67 Scassa, *supra* note 62.
68 *Supra* note 40, s 10.1.
69 *Ibid*, s 28.
70 Bill C-11, *supra* note 41.
71 Jack M Balkin, "Information Fiduciaries and the First Amendment" (2016) 49:4 UC Davis L Rev 1183 at 1209.

notes, by nature of the vulnerability those relationships engender, have a heightened duty to safeguard their clients' information.[72] In the event that a doctor, lawyer, or accountant sold information from their clients to a data broker or to gain business advantage, they would likely be found in breach of professional obligations, even in scenarios not spelled out in contract.[73] The existence of such duties indicates that "speech within these relationships [is] part of ordinary social and economic activity that is subject to reasonable regulation."[74] Thus, Balkin advocates extending these duties to data guardians through the concept of the information fiduciary.

Viewing Peoples Trust as an information fiduciary in the present scenario may alleviate the problems associated with proving unauthorized use, as mere breach of the fiduciary relationship does not require harm to create liability for damages.[75] On an intuitive level, it also seems sensible to assume that Peoples Trust has a fiduciary relationship with those who provided their data to it. Many companies handling peoples' data take this self-image to heart. As Mark Zuckerberg, the CEO of Facebook, has stated: "our own self-image of ourselves and what we are doing is that we are acting as fiduciaries."[76] Although Zuckerberg was likely using this term outside of its legal meaning, his remarks invite reading the relationship between the data subjects and the data guardians in new terms. Moreover, the existence of a fiduciary relationship may, in fact, place constrictions on the what a data guardian can do with a data subject's data, especially in the business setting where the profit motive of a corporation would then appear not to trump its responsibilities to prioritize the interests of the data subject.

And yet, prescribing a fiduciary duty to any data guardian who receives data from an individual may jump too far ahead in this particular matter. As with data breaches themselves, there is a question of degree in the duties that exist. For example, merely providing small amounts of discrete personal information may not rise to the same level as a company like Facebook possessing vast amounts of individuals' data. Similarly, there is a difference in data breaches caused by failure to take precautions compared to those caused by rogue employees already possessing access to a network. Accordingly, the responsibilities incumbent on the actor may not be the same. Moreover, many of the same objectives met by the information fiduciary construct — in particular, the articulation of specific duties around safeguarding sensitive information — can be delivered in a more limited form through the breach of confidence. Thus, a tort along the lines of a failure to take adequate precautions resulting in a data breach may be needed. In applying the breach of confidence in these scenarios, though, courts could reinforce the norms in relationships that lead individuals like

---

72 *Ibid*.

73 *Ibid* at 1205–206.

74 *Ibid* at 1217.

75 See *Lac Minerals*, *supra* note 2 at 663:

> It is clear, however, that fiduciary obligations can be breached without harm being inflicted on the beneficiary. *Keech v. Sandford* (1726), Sel. Cas. T. King 61, 25 E.R. 223, is the clearest example. In that case a fiduciary duty was breached even though the beneficiary suffered no harm and indeed could not have benefitted from the opportunity the fiduciary pursued. Beneficiaries of trusts, however, are a class that is susceptible to harm, and are therefore protected by the fiduciary regime. Not only is actual harm not necessary, susceptibility to harm will not be present in many cases.

76 Harvard Law School, "Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements" (20 February 2019) at 00h:05m:25s, online (video): <www.youtube.com/watch?v=WGchhsKhG-A>.

the putative class members in *Tucci* to provide their data to data guardians in the first place. As such transactions occur on a nearly daily basis — and, as Zuckerberg notes, since the self-image (and often the public perception) is that the data guardians should treat their responsibility vis-à-vis this data seriously, even if not quite as (legal) fiduciaries — it may be time to recognize such norms through a new legal instrument, since the contractual model has not caught up with the recognition of these norms and the statutory response has been slow.

By failing to recognize that unauthorized use might entail affirmative expectations to prevent misappropriation, especially where the misappropriation was foreseeable in light of failure to adhere to recognized safeguards, the trial and appellate Courts in *Tucci* missed a significant opportunity to create discrete liability for data guardians absconding from these recognized safeguards and abusing the trust that gave rise to individuals providing it with their data. Such a reading of the breach of confidence would have placed the emphasis less on the information itself than the relationship that caused it to be provided. In any case, the proceeding in *Tucci* concerned class certification, and few data breach cases have gone to the merits. For now, it remains to be seen whether other courts will expand the scope of this action, but the true test of the true limits of the breach of confidence in the context of data breaches will come.

[*this page is intentionally blank*]