Australian Competition and Consumer Commission v Google: Deterring misleading conduct in digital privacy policies

Jeannie Marie Paterson, Elise Bant and Henry Cooney

Introduction

Concerns over digital platforms' collection and use of consumer data, and the impact of their data practices on personal privacy, consumer autonomy and market competition, have been increasing across the globe in recent years.[1] The central business model of digital platform giants such as Google, Amazon, and Facebook, as well as relative newcomers Baidu, Alibaba and Tencent, is premised on bringing together consumers wanting to buy products and businesses wanting to advertise or sell their products to particular groups of consumers.[2] This strategy relies on 'consumer profiling', a process through which data collected from consumers' online interactions is fed into algorithms to make predictions about those consumers' future behaviour, as well as those who resemble them.[3] In data collection for profiling purposes, location data is particularly valuable.[4] Location data links consumer profiles to a physical location, which provides insights about their actual behaviour that can improve the granularity of micro-targeting and the accuracy of predictions from data analytics.[5]

In many countries, including the UK[6] and, to some extent, Australia,[7] the data collection that informs consumer profiling and targeted advertising is regulated by privacy or data protection legislation.[8] Under these regimes, either notice[9] or consumer consent[10] is a key justification for data processing. However, notice and consent requirements do not dispel all concerns about the harmful effects of consumer data processing by digital platforms. There remain further concerns about the way in which digital platforms may use insights about the psychological habits and behavioural biases of consumers, along with consumers' typical lack of interest in and knowledge of data privacy, to nudge and even manipulate consumers towards privacy-reducing rather than privacy-enhancing options in their digital interactions with the market.[11]

The emphasis in privacy and data protection law on consent as the gatekeeper to protect consumers' interests suggests that consumer protection law may here serve a valuable, additional role.[12] This body of statutory law is specifically focused on protecting consumers from conduct that impedes their decision-making, through prohibitions on misleading conduct and aggressive market practices, along with regimes scrutinising unfair contract terms.[13] In this context, the decision of the Australian Federal Court in *Australian Competition and Consumer Commission v Google*[14] (*ACCC v Google*) is potentially of great interest to other jurisdictions concerned about the strategic use of privacy notices and consent procedures to erode consumer welfare and choice. In this case, the Australian consumer protection regulator, the

Australian Competition and Consumer Commission (ACCC), successfully argued that Google engaged in misleading conduct about the steps needed to prevent Google from obtaining consumers' personal data about their location, contrary to prohibitions in the Australian Consumer Law (ACL).[15] Specifically, the Federal Court held that some reasonable users of mobile devices with Android operating systems would be misled into thinking that they could control Google's location data collection practices by switching off the 'Location History' setting on their phones. In reality, a further setting, 'Web & App Activity', also needed to be disabled to provide this protection.

The decision provides an important demonstration of the potential for courts to apply relatively longstanding consumer protection laws to new scenarios. It also illustrates the scope for the open-ended standards provided under this body of law to be informed by new insights about the way 'choice architecture', 'dark patterns' and the design and presentation of information can be used to mislead and unduly influence consumers' choices.[16] Additionally, the decision should prompt discussion about effective regulatory strategies for deterring further instances of unlawful data collection approaches. Here, a key concern is that claims for compensation for harm to consumer interests may barely make an impact on the balance sheet of digital platforms. An alternative, utilised in Australia and also available under the Data Protection Act 2018, is the use of civil penalties or fines.

Finally, in imposing civil penalties, typically a relevant consideration is the extent to which the conduct was deliberate or otherwise culpable. We suggest that the decision in *ACCC v Google* provides a strong illustration of the utility of a 'systems intentionality' approach to this question of corporate culpability. On this model, the corporate mindset is not found derivatively through individual employees, but is manifested in the systems and policies for which the corporation itself was responsible. It suggests that Google may be judged highly culpable in misleading Android phone users about privacy protections.

The Australian Consumer Regulator's Action Against Google

Risks of widespread data processing

As is probably now well recognised, while consumers do not pay a fee to access the services offered by most digital platforms, their data is the effective price of the service. There are numerous risks of harm to consumer interests from the widespread processing that forms the core business model of digital platforms.[17] These possible harms may include decreased privacy, increased risk of data breach and cybercrime, and vulnerability to scams arising through the transmission and storage of personal data. There are also risks that arise from the use of consumer data to create digital profiles which inform targeted advertising, including risks of manipulation, discrimination and exclusion from particular markets.[18] The kind of micro-targeting enabled by profiling also risks harming competition by reducing the purchasing options made visible to consumers and crowding out alternative options.[19]

In response to these risks, data protection regimes such as the General Data Protection Regulation 2016 (EU) 2016/679 ([2016] OJ L119/1) (GDPR), and the Data Protection Act 2018, impose robust requirements for valid consent to the processing of personal data. Consent must be a 'freely given, specific, informed and unambiguous indication of the individual's wishes by which they clearly signify agreement to the processing of personal data relating to him or her'.[20] By contrast, in Australia, the Privacy Act 1988, currently subject to review,[21] does not have clear or constrained limits on the collection of personal data for targeted advertising.[22] Instead, in Australia, data collection typically only requires that consumers be shown a privacy notice[23] and, where consent to data collection practices is necessary, the Australian Privacy Act allows that consent to be express or implied.[24]

Privacy advocates and scholars have long warned against over-reliance on consent to protect consumers' interests.[25] This is because consumers are typically too busy to take the time to read privacy policies, and lack the legal expertise to make much sense of them. Moreover, even if consumers devote time to such provisions, these are commonly long, complex, vague, and difficult to navigate.[26] Consumers operate under conditions of bounded rationality or cognitive bias, which further limit their capacity to make sense of large amounts of information and multiple choices between different privacy options. This reality presents a key role for consumer protection law to buttress the protection provided by privacy regimes by further safeguarding the circumstances in which consumers are asked to consent to proposed data collection and use.[27] Consumer protection law is precisely focused on the process through which consent is obtained, using prohibitions on misleading conduct and undue

influence or pressure,[28] as well as regulating the substantive fairness of the terms to which consumers are asked to agree through unfair terms regimes.[29]

As already noted[30] and discussed in more detail below,[31] firms may seek to influence, mislead or manipulate consumers' consent to data collection, processing and use through the way in which the information is displayed, organised and presented in context. These design strategies, sometimes described as choice architecture or dark patterns, appear to be widespread in online transactions. Notably, a 2020 study found that dark patterns and terms reliant on implied consent were ubiquitous on the most popular 10,000 websites in the UK.[32] Such practices threaten to undermine the integrity of consumer consent to notices that set out the data-processing practices of digital platforms and online firms.[33]

Concerns about this kind of conduct has led regulators in several jurisdictions to take action against digital platforms. In Australia, the focus of this article, the ACCC has been successful in an action against Google for misleading consumers over the steps needed to preclude location tracking in Android phones, in contravention of the statutory prohibition on misleading conduct under the ACL.[34] The core Australian prohibition, contained in s 18 of the ACL, goes beyond prohibiting positive misrepresentation to capture any misleading 'conduct'. The overall effect of 'conduct' is broadly construed, including silences, omissions and the overall presentation of information.[35] In the UK, the equivalent prohibitions are regs 5 and 6 of the Consumer Protection from Unfair Trading Regulations 2008, implementing the EU Unfair Commercial Practices Directive 2005/29/EC ([2005] OJ L149/22), which ban misleading practices and omissions.[36]

We further note that a more direct avenue of response may be under statutory unfair trading or transparency requirements, given the core concern is over salient information that may be technically present but unrealistic for consumers to access because it is, for example, buried under multiple navigation screens.[37] Thus, the use of choice architecture to guide consumers to decision outcomes that favour the provider of the services to the disadvantage of the consumer may infringe the general prohibition on unfair trading in reg 3 of the Unfair Trading Regulations 2008.[38] Where the design of privacy settings makes it difficult for consumers to navigate, or nudge consumers towards certain privacy-eroding options, there may also be a contravention of the robust requirements for valid consent under the GDPR and the Data Protection Act 2018.[39] In the US, the Federal Trade Commission has signalled a willingness to apply s 5 of the Federal Trade Commission Act 1914 to privacy-eroding practices of this kind. The Federal Trade Commission recently fined Facebook 5 billion USD for misrepresenting the extent to which its users could control access to their personal data.[40]

As is discussed further below, however, prohibitions on misleading conduct may be a useful starting point for responding to manipulative design practices. Moreover, the availability of any regulatory response, will depend upon a careful analysis of both the design of the choice options and the way in which the relevant information (as presented to the consumer) can mislead or unduly influence consumer decision-making. In this regard, *ACCC v Google* offers a particularly salient case study of the potentially powerful legislative and regulatory strategies that may be deployed against such practices.

Misleading conduct in presenting privacy control options

ACCC v Google arose in the context of alleged contraventions of various prohibitions on misleading conduct in the ACL by Google between January 2017 and December 2018. The impugned conduct related to the way Google accessed, retained and used the personal location data of users of Android mobile devices. For current purposes,[41] the ACCC's case against Google centred upon the content of various screens that Android users saw when they sought to control access to their personal data.[42] Two settings were central to the ACCC's case. The first was a setting called 'Location History'. This setting was described as controlling whether Google could save a 'private map' of the user's location data.[43] The second was a setting called 'Web & App Activity'. This setting purported to control whether Google could save a user's searches, browsing history, and activity within Google apps and services.[44] The default setting of 'Location History' was 'off', whereas 'Web & App Activity' was set by default to 'on'.[45] As it turned out, *both* settings controlled Google's access to personal location data. Thus even with 'Location History' set to 'off', the default setting of 'Web & App Activity' to 'on' meant that Google could access, retain and exploit a user's personal location data when the user used certain apps and services. The personal data collected by Google, including location data, was used for a variety of purposes, including by the users of Google services and also for personalised advertising and the sale of advertising services to third parties.[46]

The Federal Court found that Google's conduct was misleading or likely to mislead, in contravention of s 18 of the ACL. The Federal Court also found that Google had misled users about the nature, characteristics or suitability for purpose of Google services accessed by Android mobile device users, which contravened the more specific prohibitions contained in s(s) 29(1)(g)[47] and 34[48] of the ACL respectively.

In bringing its case, the ACCC acknowledged that the majority of users would not have clicked past the Privacy and Terms screen on their device to the screen titled 'More Options' where the problematic settings were located.[49] Instead the ACCC conducted its case by reference to three classes of users of Android mobile devices.[50] Scenario 1 concerned users who had considered the 'Location History' and 'Web & App Activity' settings while setting up their mobile devices.[51] Scenario 2 concerned users who had consciously decided to turn 'Location History' to 'off' (after having previously switched it to 'on').[52] Scenario 3 concerned users who, after setting up their device, had consciously considered whether to change 'Web & App Activity' from its default setting of 'on' to 'off'.[53]

In each of the three scenarios considered by the court, accessing the 'Location History' or 'Web & Activity' settings required consumers to navigate through various screens. For example, the hypothetical class of users in 'Scenario 1' were users who, while setting up their device, scrolled through Google's privacy policy and, instead of pressing 'I agree' or 'Don't create the account', pressed a 'More Options' button (itself found underneath the heading 'You're in control'). Upon pressing 'More Options', the user was shown the 'Location History' and 'Web & App Activity' settings. Both settings were accompanied by a 'Learn more' link, though neither link informed the user that, despite turning 'Location History' to 'off', personal location data would still be collected when the 'Web & App Activity' setting was enabled. The second and third scenarios also involved users who had navigated through the settings of their mobile device: Scenario 2 concerned users who had found their way to the 'Location History' setting, while Scenario 3 concerned users who had found their way to the 'Web & App Activity' setting.

Australian courts have a well-developed jurisprudence around assessing when conduct directed to the public, as opposed to an individual person, is misleading. When conduct is directed toward the general public, or a section of the general public, the approach of the court involves considering the effect of the conduct upon reasonable members of the class of people to whom the conduct was directed.[54] In considering how a hypothetical, reasonable member of the relevant class would have responded, the court allows for different responses from different reasonable members of the class. It is not to the point that some members of the relevant class would not have been misled, because the court does not need to 'land upon one response'[55] or distil the class 'into a single hypothetical reasonable person'.[56] It is enough that some members of the relevant class would, acting reasonably, have been misled.[57]

In *ACCC v Google*, the Federal Court held that even though there were potentially tens of thousands of users within each class, the relevant users within each class were those likely to pay some attention to the settings information shown to them.[58] This is because each of the three scenarios involved a deliberate decision to seek out the privacy settings – something the 'average' user (a user without some reason to access the settings, such as a particular interest in privacy or data-protection) would be unlikely to do.[59] The Federal Court found that while Google's conduct would not have misled all users of Android devices in the relevant time period, it would have misled (or the conduct would have been likely to mislead) some reasonable users within the classes identified.[60] This was sufficient to establish a contravention of the relevant provisions in the ACL.

Insights from behavioural economics

Although lauded by privacy advocates, the finding in *ACCC v Google* that some users had been misled deserves further attention. This conclusion relied on the court going beyond the mere presence of relevant information, to gain a more holistic understanding of the user experience. Information disclosing what was collected by Google, and what needed to be disabled to prevent this collection, was available through a close analysis of the various screens. For example, Google's general Privacy Terms referred to it collecting location data.[61] For those consumers who went further and navigated past the Privacy Terms to 'More Options', Google did not expressly misrepresent that disabling 'Location History' would prevent Google from using any of a user's location data. Further, Google had never explicitly represented that Google would not be able to use a user's location data even if 'Web & App Activity' were enabled.[62] Users had the opportunity to go further into the terms and conditions, by clicking on a 'Learn More' link. This link provided more information about the

data collected when the relevant settings were on, including an express statement under 'Web & App Activity' that data saved when this option was switched on included 'your location and other associated data'.[63]

A key reason Google's conduct was held to be misleading, despite the formal availability of the relevant information, turns on the preparedness of the court to consider evidence about behavioural psychology and an understanding of the way in which the choices that were presented to consumers influenced their decision-making. Both Google and the ACCC relied on expert evidence from economists with expertise in 'behavioural economics',[64] which is the study of human decision-making informed by psychology and without accepting the precept of perfect rationality relied on in classical economic theory.[65] The experts explained that analysis of how users navigated various screens in making decisions about privacy should be informed by a realistic understanding of the impact of limited time and of various behavioural biases on consumer decision-making processes:[66]

> *Behavioural economics starts from the premise that people are time constrained, do not have all (or even most) information easily accessible and have cognitive capacity with serious limits in processing information when making choices. These constraints cause people to use short-cuts (referred to as 'heuristics') to make choices. The heuristics are subject to many biases, which result in systematic and predictable deviations from making the optimal choices which would be assumed in the traditional economic approach. Behavioural economists would say that people are 'boundedly rational'.*[67]

Against this backdrop of bounded rationality, the expert economists also gave evidence on the influence of choice architecture on consumer decision-making.[68] Choice architecture refers to the ways in which the design and presentation of information may influence the choices that are made by individuals, particularly given the potential for those processes to leverage behavioural biases in consumer decision-making. An application of this process is the use of dark patterns in the design of privacy consent procedures or notices.[69] Dark patterns use behavioural biases in the design of websites and other digital interfaces to influence consumers to make decisions that benefit the firm deploying the technology, to their own detriment.[70] Examples of the use of choice architecture or dark patterns include default options that are set to privacy intrusive options, which plays on natural consumer inertia;[71] making 'opting out' of privacy-eroding options or memberships cumbersome by increasing the number of clicks needed to complete the action;[72] framing the effects of options for choice in terms of positive words and images and underplaying negative outcomes of that choice;[73] and using headings and other attention-catching designs to make certain information salient to consumers, while diverting attention from other options.[74]

The expert economists agreed that behavioural economics alone could not predict the reaction of consumers to the screens displayed to them when investigating the privacy settings on their phones.[75] However, the expert economists' evidence about behavioural economics does appear to have influenced the Federal Court's reasoning as to why the information presented was misleading to at least some of the relevant class of consumers. We can explain the finding in terms of these behavioural insights through the following reasoning. Generally, behavioural economics supports the view, long recognised by consumer protection advocates, that merely providing information relevant to consumers' decisions somewhere on a website or phone screen is not sufficient to ensure that information is salient in informing those decisions.[76] Specifically, in the circumstances raised by *ACCC v Google*, this insight means that information available to consumers through the 'Learn More' option was not necessarily sufficient to counter the misleading impression gained from the labelling of the 'Location History' and 'Web & App Activity' settings. This impression was that 'Location History' was the pertinent setting to disable location tracking. Accordingly, the fact some consumers wielding a 'high degree of observation'[77] might conceivably have drawn the correct conclusion as to location tracking from clicking through and reading further screens was not alone sufficient to protect Google's conduct from being misleading.

As already noted, the ACCC's case was based on atypical users who were sufficiently concerned about privacy to navigate to the 'More Options' screen.[78] The Federal Court accepted that reasonable members of the relevant category of users would not have paid close attention to the detail of the information provided at that point, having regard to what preceded it, and the possibility of finding out more by clicking further.[79] The Federal Court accepted that an atypical user who navigated to the 'More Options' screen and saw the default settings may have been misled, because at that point they

were not expressly notified that, even if 'Location History' was off, Google might continue to obtain, retain and use personal location data.[80] On this view, given that only the setting 'Location History' referred to location, it was reasonable for users to assume this was the only relevant setting that controlled access to location data.[81] Implicit in this position was that it was reasonable for an Android phone user who sought to find out more about privacy options not to navigate past 'Other Options' to 'Learn More', at which point the true situation would have been revealed.[82] Also important in the courts' reasoning was the recognition, drawn from an understanding of choice architecture, that the atypical user investigating the 'More Options' screen may reasonably have focused on the heading 'Location Settings', and the option of switching off this option, and may not have further investigated other controls over location tracking.[83]

Thus, overall, and perhaps uniquely in judgments about the scope of consumer protection legislation, the court in *ACCC v Google* assessed whether conduct was misleading by reference to a consumer who was boundedly rational, rather than the benchmark 'average' consumer of EU jurisprudence who is 'reasonably well-informed and reasonably observant and circumspect'.[84] In the words of Thawley J:

> *A user particularly paranoid about having his or her location used might have clicked on 'Learn more' underneath Web & App Activity despite there being no reference to 'location' connected to that setting on the More Options screen. Others may have too. However, I am satisfied that there were reasonable users who had clicked on 'More Options', who would choose not to continue and click on each of the 'Learn more' links or one or other of them. There is a point where reasonable people give up drilling down to plumb the depths for further information. I would think the lack of desire increases with each link.*[85]

Using civil penalties to deter wrongful conduct

Civil penalties as an enforcement tool

Breaches of the prohibition on misleading conduct in the ACL give rise to liability to pay damages to consumers who have suffered loss or damage because of the misleading conduct,[86] and also to the possibility of broader compensatory and 'non-punitive' orders.[87] Additionally, the Australian regulator, the ACCC, has extensive enforcement powers in relation to these prohibitions. The ACCC has power to issue infringement notices and enter into enforceable undertakings. It can also go to court to seek compensation on behalf of consumers who have suffered loss and damage, bring criminal prosecutions, and seek civil pecuniary penalties for contraventions of the law.[88] Two of the three provisions that Google breached are provisions subject to the civil penalty regime under the ACL. This means that for each of Google's contraventions (of which there could be thousands) the court may impose a penalty of up to 1.1 million AUD.[89]

The ACCC has made particular use of the civil penalty regime in responding to contraventions of the ACL, and in seeking to effect both specific and general deterrence. Unless Google appeals the liability judgment, a penalty hearing will be the next step in the ACCC's enforcement action in this case. Currently, civil penalties or fines are not available as an option for contraventions of the UK's equivalent consumer protection regime under either the Unfair Trading Regulations 2008 or the Consumer Rights Act 2015. Notably, the UK government announced a process of consultation in 2019 on whether the Competition and Markets Authority (CMA) should be given new powers to decide whether consumer law has been broken, without having to go through the courts, and to impose fines directly in response to such conduct. It would appear that little progress has been made on this inquiry. Civil penalties are, however, available under the DPA 2018 for contraventions of its provisions and the GDPR,[90] and may be imposed directly by the regulator itself.[91]

The primary goal of the pecuniary penalty regime in the ACL is deterrence;[92] this is similarly listed as an objective of the DPA 2018.[93] This goal encompasses both 'specific' deterrence (discouraging the defendant from committing further contraventions) and 'general' deterrence (discouraging members of the public from committing contraventions).[94] The Federal Court has explicitly recognised that correct calibration of the penalty is central to achieving deterrence. Among other matters, courts have emphasised that any penalty should not be so low that it becomes merely a 'cost of doing business'.[95] Indeed, so great is this concern that the minimum penalties payable have recently been increased in Australia. The goal of deterrence suggests that Google – a multi-national, trillion-dollar company with annual revenues in the hundreds of billions – should receive a significant penalty.

Specific factors relevant in setting the penalty are set out in the legislation[96] and also have been developed by courts.[97] The legislation directs courts to consider

the nature and extent of the misleading conduct, the loss or damage to consumers and the circumstances of the contravention.[98] In addition, courts will have regard to a number of general law factors, including the size of the contravening company, past conduct, whether the contravention arose from the conduct of senior management, the cooperation shown by the defendant after the conduct was identified, and whether the contravening conduct was systematic, deliberate or covert.[99] More recently, courts have suggested that it is also relevant to consider the profit made from the contraventions.[100] Similar considerations are listed as influencing the level of fine payable under the DPA 2018, including specifically the 'intentional or negligent character of the failure',[101] 'the degree of responsibility of the controller or processor',[102] 'the degree of co-operation … in order to remedy the failure and mitigate the possible adverse effects of the failure'[103] and 'any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly)'.[104]

While the goal of civil penalties is deterrence, in considering these factors, courts also show a concern to ensure that the penalty is not a crippling burden[105] and is commensurate with the defendant's level of wrongdoing.[106] At this point, Google might argue that only some out of many consumers of its services were misled and, moreover, that its contraventions of the law were unintentional. These factors might seem to reduce the seriousness or at least the moral culpability of the misconduct. But we consider that these factors should not unduly cap any penalty awarded in this case.

In *ACCC v Google*, the number of consumers misled by Google's conduct will be difficult to assess. As the court pointed out, many consumers would not have checked their privacy options.[107] But even if only a proportion of Android users were misled, that will remain a very large number.[108] Relevantly, there was evidence before the Federal Court that, after press reports of the location tracking problem, the number of consumers switching off the 'Web & App' option increased by 500 per cent. We may further accept that, even if a court is able to find that the potential number of affected consumers is large, the level of harm from this conduct is highly amorphous, given it involves non-pecuniary harms to fundamental rights of privacy and autonomy.[109] Nonetheless, it is also clear that Google profits extensively from these data harvesting practices. Google's very business model is premised on monetising consumer engagement or attention through advertising services.[110] Consumer data has considerable market value. This needs to be acknowledged and factored into the size of the penalty, lest the offending conduct be subsumed as a mere cost of doing (very good) business.

Australian courts have consistently assessed 'deliberate, covert or reckless conduct, as opposed to negligence or carelessness,'[111] as more serious, and liable to attract a significantly higher penalty.[112] Here, Google will no doubt argue (and appears to have already argued[113]) that the misleading design of the privacy settings was not deliberate, but rather the result of a mere oversight on its part. Consistently with this narrative, it was revealed at trial that individual Google employees responsible for oversight of the various privacy settings were not aware of the problem until the Associated Press published an exposé[114] critical of the confusing nature of the 'Location History' and 'Web & App Activity' settings.[115] The Associated Press article prompted an urgent meeting of these employees, at which it was resolved to remedy the issue and 'reduce user confusion [regarding] how location [data] is used across [Google] products and services'.[116]

Our view is that, in setting the appropriate level of penalty, the fact Google employees were initially and personally ignorant of the misleading nature of Google's privacy settings should be largely irrelevant in the assessment of Google's corporate state of mind.[117] This is because Google's corporate intentionality, and broader corporate state of mind, is manifested in, and revealed by, the systems that Google designed and put in place. Arguably, these systems indicate that Google's conduct was both knowing and deliberate. To understand the grounds for, and significance of, this assessment, it is necessary to address the limits of, and more recent developments upon, traditional rules of corporate attribution.

Corporate responsibility and 'systems intentionality'

Enquiries into a defendant's state of mind are widespread throughout the law, arising as a condition of primary liability for many species of legal and equitable wrongdoing.[118] A defendant's state of mind may also influence remedial outcomes[119] and bear on defences.[120] As we have seen, state of mind is also key to setting pecuniary penalties, through concepts such as deliberateness and, by way of mitigation, contrition. This is so even where (as with Australia's wide-ranging statutory prohibitions on misleading conduct) primary liability is strict.

Against this background, it is of increasing concern that the law's approach to enquiries into state of mind may be fundamentally inapt when dealing with large corporations.[121] Traditionally, whether a corporation intended an act, or had knowledge of a particular matter, turned upon an enquiry into whether the corporation's board of directors, or senior delegates of the board (the corporation's 'directing mind and will') had the relevant intention or knowledge.[122] A more nuanced approach, developed first by the House of Lords in *Meridian Global Funds Management Asia Ltd v The Securities Commission Co*,[123] and adopted in some common law jurisdictions,[124] involves tailoring the attribution enquiry by reference to the particular rule of liability or proscription that is in focus.[125] In other words, the purpose of a particular prohibition might mean that it is not necessary to enquire into the state of mind of the corporation's directors or senior managers – the prohibition itself will dictate which officer or employee's state of mind counts for the purposes of the attribution enquiry.[126] However, while this approach has gone some way to address the restricted nature of the 'directing mind and will' test, it is still generally dependent on identifying a relevant individual whose state of mind may be properly attributed to the company. A similarly derivative approach to corporate liability can be seen in most statutory provisions addressing corporate misconduct, both in Australia[127] and in the United Kingdom.[128]

A major problem with these approaches is that a corporation's conduct does not always neatly 'match up' to the decision-making of individual employees. In large, complex corporations, it is common for tasks to be widely delegated and for knowledge to be 'siloed' within teams and fragmented across multiple individuals.[129] Further, individual employees may have little understanding of how their allocated task fits with the broader corporate agenda: they are simply 'doing their job'. The reality of 'diffused responsibility'[130] within corporations makes human-focused attribution enquiries difficult, and encourages both deliberate and unintentional evasion of corporate responsibility. More fundamentally, a corporation's behaviour is often 'the product of organizational policies and collective procedures, not individual decisions'.[131] When this is the case, it will not even make sense to try to identify particular employees on which to hang the corporation's state of mind – any fault must be found within the corporation's systems themselves. This conclusion is only fortified when viewed in light of the increasing reliance of corporations upon automated systems and artificial intelligence platforms,[132] both of which can result in a corporation acting with little or no ongoing human input.

Google exemplifies these sorts of problems. Google is one of the largest companies in the world, with almost 150,000 employees spread across 50 countries. In the case in question, Google employees across different teams were involved in the design of the privacy settings, including software engineers, product managers, consultants, and members of Google's public affairs division.[133] There is no evidence that individual employees deliberately set out to mislead users of Android mobile devices in the design of the 'Location History' and 'Web & App Activity' settings. On a traditional approach to corporate attribution, we might therefore conclude that Google's conduct in misleading users was not deliberate, but instead accidental or the result of inattention. However, this approach would overlook the fact that leading users of Android mobile devices into error was precisely the sort of result that Google's choice architecture was apt to produce.

This brings us to an emerging approach to corporate culpability, in which a corporation's state of mind is manifested in the corporation's systems, policies and patterns of behaviour.[134] Central to this approach is recognition that the ethical quality of a corporation's behaviour – its organisational blameworthiness – must be assessed by reference to the actions of the corporation itself, even in the absence of individual human fault.[135] This is not to deny that the state of mind of a corporation is often referable to the state of mind of the corporation's natural agents – there is no difficulty in labelling a corporation's conduct dishonest, for example, when the corporation's directors set out to act dishonestly. The directors, after all, form one of the primary processes for corporate decision-making. The important point is that a corporation can *also* manifest states of mind independently of any human individual. That is, a corporation's state of mind can be found within broader systems and processes adopted and implemented by the corporation to achieve its ends.

On this understanding, corporate systems are inherently purposive, being internal methods or organised connections of elements operating to produce conduct.[136] Beyond its internal structures and processes, the corporation's systems, and through them its state of mind, may be evidenced through the corporation's objectively discernible patterns of behaviours and habitual practices. Further, a corporation may be taken to know the essential

features of its adopted systems and what is required for each system to function. For example, a significant corporation like Google must be taken to know that its privacy settings set default choices, and that these defaults inevitably have implications both for consumers and for related corporate income-generating, data-driven activities. On this account, if a corporation designs and implements a system apt to produce a particular outcome, that outcome cannot be dismissed as accidental or unintentional. The design and implementation of the system is *itself* a manifestation of the corporation's intent.

Returning to *ACCC v Google*, the fact that some employees were not personally aware of the location tracking problem does not mean that Google was correspondingly ignorant and, hence, devoid of relevant knowledge or intention. Google designed and operated the information system that faced consumers trying to manage their privacy settings. It was Google that set the screen contents and layout, and it was Google that set the default settings. The overall data-harvesting system, as implemented, reflected and instantiated Google's own design choices, aims and preferences. Consistently, the resultant choices offered to consumers effectively steered them away from opting out of Google collecting, retaining and using valuable personal location data. Not only did the 'Other Options' information fail to refer to the fact that location tracking was carried out via processes other than the one labelled 'Location History'. The default option for 'Web & App Activity' (which included location tracking) was set as 'on'. The individual Google employees may not have directed their attention to these details. But that is not to the point. Google's corporate mindset is manifested or revealed in the systems it designs and put in place. This privacy-eroding system arose by design not accident. It therefore warrants a serious penalty.

Conclusion

ACCC v Google is significant in a number of respects: as an illustration of a robust approach to enforcement by a consumer protection regulator; for its use of the insights of modern learning about consumer decision-making that may be affected by the design of privacy policies; and in prompting scrutiny of the degree of culpability that should be attributed to Google for its misleading conduct. The pragmatic question that remains is whether the action of a single regulator in a small market economy can realistically have any impact on the business practices of a company the size of Google. Our observations here are four-fold.

First, consumer protection law provides insights into the ways in which consumer choice may be eroded by conduct that is misleading or manipulative, including in the way in which choice options are designed. Whether enforcing data protection or consumer protection laws in the digital context, it is vital for regulators and decision-makers to understand the ways in which the very architecture of notice provisions may influence, nudge and even manipulate consumer decision-making. Intrinsic to this is recognition of the reality of the low degree of close attention reasonable consumers are likely to bring to such processes. Secondly, while it may seem a piecemeal approach to tackle concerns about the privacy-eroding effect of consumers' interactions with digital platforms through focusing on the transparency and accuracy of privacy policies, regulators' use of civil penalty provisions that attach to contraventions of consumer or privacy/data protection law can lend greater weight than relying on individual actions by consumers. Thirdly, regulators increasingly can, if they so choose, impose significant penalties for contraventions that have the potential for deterrence by eating into corporate profit. Indeed, we note it is possible to envisage a cross-border effort where regulators in different jurisdictions coordinate enforcement strategies, by comparing and sharing evidence and approaches. Fourthly, effective use of civil penalty regimes to deter harmful conduct should be informed by a robust theory of corporate culpability that understands the role of systems in attributing intentionality to corporate behaviour. This form of analysis both enables a principled assessment of corporate blameworthiness and provides a practical impetus for corporations to take seriously their responsibility for introducing and maintaining fair digital business practices.

Jeannie Marie Paterson
Professor of Law, Co-Director of the Centre for Artificial Intelligence and Digital Ethics, The University of Melbourne.

Elise Bant
Professor of Private Law and Commercial Regulation, The University of Western Australia, and Professorial Fellow, The University of Melbourne.

Henry Cooney
JD Candidate and Research Associate, University of Western Australia.

Notes

1 See generally the Australian Competition and Consumer Commission, *Digital Platforms Inquiry*: *Final Report* (2019) at p 1; United Kingdom Government, *Online Harms White Paper: Full Government Response to the Consultation* (Consultation Outcome, 2020) <https://www.gov.uk/government/consultations/online-harms-white-paper> last accessed 1 July 2021.
2 Supra (Digital Platforms Inquiry) n 1 at 41.
3 See further Forbrukerrådet, *Out of Control* (Research Report, 14 January 2020) ch 2; Salinger Privacy, *Cookies and Other Online Identifiers: Research Paper for the Office of the Australian Information Commissioner* (15 June 2020); S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
4 Supra (Digital Platforms Inquiry) n 1 at 385.
5 Supra (Salinger Privacy) n 3 at 46–47.
6 See the Data Protection Act 2018.
7 Privacy Act 1988 (Cth).
8 Perhaps the most prominent regime is the General Consumer Data Protection Regulation 2016/679 (GDPR).
9 Privacy Act 1988 sch 1 APPs 1, 5.
10 GDPR art 6(1); Data Protection Act 2018 s 2(1)(a).
11 See generally K Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design' (2016) 20(1) Information, Communication & Society 118.
12 S Corones and J Davis, 'Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions' (2017) 45 Federal Law Review 65; D Clifford, I Graef and P Valcke, 'Pre-formulated Declarations of Data Subject Consent – Citizen-consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2019) 20 German Law Journal 679.
13 See further discussion in D Clifford and J M Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94(10) Australian Law Journal 741.
14 [2021] FCA 367.
15 Competition and Consumer Act 2010 (Cth) sch 2 (ACL).
16 Forbrukerrådet, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (Research Report, June 2018); Sebastian Rieger & Caroline Sinders, *Dark Patterns: Regulating Digital Design* (Stiftung Neue Verantwortung, 2020); Commission nationale de l'informatique et des libertés, *Shaping Choices in the Digital World* (Research Report, January 2019).
17 On the harms to consumers of widespread data collection see in particular E Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8 Law, Innovation and Technology 1; G Wagner, 'Down by Algorithms? Siphoning Rents, Exploiting Biases and Shaping Preferences the Dark Side of Personalized Transactions' (2019) 86 University of Chicago Law Review 581; Competition and Markets Authority, United Kingdom Government, *Algorithms: How they can reduce competition and harm consumers* (Research Report, 19 January 2021) <https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers> last accessed 1 July 2021.
18 M McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) Monash University Law Review 1, 6–9.
19 See K Kemp, 'Concealed data practices and competition law: why privacy matters' (2020) 16(2–3) European Competition Journal 628.
20 GDPR recital 32, art 4(11); Data Protection Act 2018 s 84(2).
21 Attorney-General's Department, Australian Government, *Privacy Act Review: Terms of Reference* (30 October 2020) <https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-terms-reference> last accessed 1 July 2021.
22 Supra (Digital Platforms Inquiry) n 1 at 437.
23 Privacy Act 1988 sch 1 APPs 3, 6.
24 *Ibid* s 6(1).
25 Supra (Clifford and Paterson) n 13; Supra (McDonagh) n 18; D Hirsch, 'From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics' (2020) 79(2) Maryland Law Review 439.
26 Supra (Digital Platforms Inquiry) n 1 at 403–404.
27 Supra (Corones and Davis) n 12.
28 See eg Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277) pt 2; ACL ss 18 and 21.
29 See eg Consumer Rights Act 2015 pt 2; ACL pt 2–3.
30 See above text to n 16.
31 See below text to n 64 and following.
32 M Nouwens et al, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (Conference Paper, Computer-Human Interaction Conference, 2020). See also A Mathur et al, 'Dark patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM Human-Computer Interaction 81.
33 See also L E Willis, 'Deception by Design' (2020) 34(1) Harvard Journal of Law & Technology 115, discussing the challenges for regulators in responding to dynamic, micro targeted terms and conditions online.
34 Supra n 14. See also the action for misleading consumers in changing privacy terms: <https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data> last accessed 1 July 2021.
35 *Demagogue Pty Ltd v Ramensky* (1992) 39 FCR 391 at 41, *per* Gummow J.
36 The Italian Competition Authority issued a 10 million EUR fine against Facebook over data-sharing between Facebook and WhatsApp as an aggressive practice to induce consumers to allow sharing of data: Italian Competition Authority, 'Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes' (Press Release, 7 December 2018) <https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes> last accessed 1 July 2021.
37 See generally supra n 25 (Hirsch).
38 See also C Keegan and C Schroeder, 'Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms' (2019) 15(1) Journal of Law, Economics & Policy 19; J Laux, S Wachter, B Mittelstadt, 'Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice' (2021) 58(3) Common Market Law Review 719.
39 The French data protection authority imposed a 50 million EUR penalty against Google under the GDPR for violating the obligation of transparency and the obligation to have a legal basis for processing personal information: Commission nationale de l'informatique et des libertés, 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC' (Press Release, 21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-

euros-against-google-llc> last accessed 1 July 2021. See also supra (Commission nationale de l'informatique et des libertés) n 16; supra (Forbrukerrådet) n 16 at p 9.

40 Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook' (Press Release, 24 July 2019) <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> last accessed 1 July 2021. See also C Keegan and C Schroeder, 'Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms' (2019) 15(1) Journal of Law, Economics & Policy 19.

41 The court dismissed a further argument by the ACCC that consumers reading Google's privacy statement would be misled into thinking that personal data was collected to benefit them not for Google's commercial benefit: supra n 14 at [333]. Given the balance of the court's reasoning, and the expert evidence on which it rested, discussed below, this is surprising and might deserve further attention from Australian regulators concerned to protect consumers from openly, or secretly, 'data harvesting' for profit.

42 Ibid at [15], where it was noted that the ACCC ran its case 'on the basis of numerous variations of screens presented to users over various and overlapping time periods', summarised in an 'aide memoire' attached to the decision.

43 Ibid at [157]. See also [159], [233]–[234], [245], [256], [267], [279], [282]–[283].

44 Ibid at [155]. See also [233], [309]–[313].

45 Ibid at [2], [31]–[32].

46 Ibid at [38].

47 Section 29(1)(g) prohibits 'false or misleading' representations about the 'sponsorship, approval, performance characteristics, accessories, uses or benefits' of goods or services.

48 Section 34 prohibits conduct in trade or commerce that is liable to mislead the public as to the nature, the characteristics, the suitability for purpose or the quantity of any services.

49 Supra n 14 at [5].

50 Ibid at [3].

51 Ibid at [4].

52 Ibid at [7].

53 Ibid at [11].

54 *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* (1982) 220 CLR 191 at 199, *per* Gibbs CJ.

55 Supra n 14 at [98].

56 Ibid at [91]. See also *National Exchange Pty Ltd v Australian Securities and Investments Commission* (2004) 49 ACSR 369 at 375–376 [24], *per* Dowsett J; *Comité Interprofessionnel du Vin de Champagne v Powell* (2015) 330 ALR 67 at 104 [171], *per* Beach J.

57 The likelihood that some consumers would reasonably be misled differed as between the provisions. In *ACCC v Google*, the court held that while a contravention of section 18 could be shown by proving the conduct was 'likely to mislead', section 29(1)(g) and section 34 require more than a 'real or not remote chance or possibility' that a hypothetical, reasonable member of the relevant class was misled: supra n 14 at [119]–[120], [125]–[126].

58 Ibid at [138], [142]–[150], [230]–[238], [304]–[308].

59 Note, however, Thawley J's comment that 'there is no neat dividing line between typical and atypical users': ibid at [139].

60 Ibid at [17].

61 Ibid at [169].

62 Indeed, Google submitted that the use of data described under the leading 'Web & App Activity' was sufficiently broad to include location data: ibid at [188].

63 Ibid at [161].

64 Ibid at [50].

65 Ibid at [52].

66 See also supra (Digital Platforms Inquiry) n 1 at 395–396; Y Hermstrüwer, 'Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data' (2017) 8(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 9.

67 Supra n 14 at [52].

68 Ibid at [62].

69 The term 'dark patterns' was introduced by Harry Brignull, whose research can be found at <https://darkpatterns.org/> last accessed 1 July 2021. See also W Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018).

70 See further supra (Digital Platforms Inquiry) n 1 at 399–434; supra (Forbrukerrådet) n 16 at 7; supra (Rieger and Sinders) n 16.

71 Supra (Digital Platforms Inquiry) n 1 at 13–14.

72 Supra n 14 at [63]; supra (Forbrukerrådet) n 16 at 19–20.

73 Supra (Forbrukerrådet) n 16 at 22–23.

74 Supra n 14 at [63].

75 Ibid at [64].

76 See eg U Benoliel and S I Becher, 'The Duty to Read the Unreadable' (2019) 60(8) Boston College Law Review 2255; J M Paterson, 'The Australian Unfair Terms Law: The Rise of Substantive Unfairness as a Ground for Review of Standard Form Consumer Contracts' (2009) 33(3) Melbourne University Law Review 934.

77 Ibid at [203].

78 Both experts agreed that the majority of users would not pay much attention to the privacy settings on their Android phones: ibid at [136]. See also supra (Digital Platforms Inquiry) at 403, noting that the average length of privacy policies is between 2500 and 4500 words, and that it would take the average reader between 10 and 15 minutes to read a typical privacy policy.

79 Supra n 14 at [207]. See also [238], [254], [272], [322].

80 Ibid at [164].

81 Ibid at [165]

82 Ibid at [163], [213].

83 Ibid at [196], [201].

84 *Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurt* C-210/96 [1998] ECR I-4657. See also *Verbraucherschutzverein v Sektkellerei Kessler* C-303/97 [1999] ECR I-513; *Estée Lauder Cosmetics v Lancester Group* C-220/98 [2000] ECR I-117; Unfair Commercial Practices Directive 2005/29/EC ([2005] OJ L149/22) rec 18. See also Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277), reg 2(2).

85 Supra n 14 at [210].

86 ACL s 236.

87 Ibid ss 237, 246, 247.

88 Ibid pt 5–2 div 1.

89 The *ACL* penalty regime has been the subject of recent amendment. The present maximum fine for corporate breach of either section is the greater of: A$10,000,000; the value of the benefit obtained by the body corporate from the breach; or if the court cannot determine the value of the benefit attributable to the breach, 10 per cent of the annual turnover of the body corporate: ibid s 224(3A). However, Google's misleading conduct occurred before these changes came into effect, when the maximum penalty was A$1.1 million.

90 Data Protection Act 2018 s 155.

91 Ibid s 155(1).

92 *Trade Practices Commission v CSR Ltd* [1991] ATPR ¶ 41-076, at 52,152, *per* French J.

93 Data Protection Act 2018 s 155(3)(l): 'whether the penalty would be effective, proportionate and dissuasive'.

94 *Australian Building and Construction Commissioner v Construction, Forestry, Mining and Energy Union* (2018) 262 CLR 157 at 185 [87], *per* Keane, Nettle and Gordon JJ.

95 *Singtel Optus Pty Ltd v Australian Competition and Consumer Commission* (2012) 287 ALR 249 at 266 [68], *per* Keane CJ, Finn and Gilmour JJ.
96 ACL s 224.
97 See in particular *Trade Practices Commission v CSR Ltd* [1991] ATPR ¶ 41–076. For a recent summary of the factors, see *Australian Competition and Consumer Commission v B & K Holdings (Qld) Pty Ltd* [2021] FCA 260 at 14–17 [80], *per* Derrington J.
98 ACL s 224(2). See also *Australian Competition and Consumer Commission v Reckitt Benckiser (Australia) Pty Ltd* (2016) 340 ALR 25 at 41–50 [59]–[98], *per* Jagot, Yates and Bromwich JJ.
99 *Australian Competition and Consumer Commission v Singtel Optus Pty Ltd [No 4]* (2011) 282 ALR 246 at 250–251 [11], referred to without demurral on appeal in *Singtel Optus Pty Ltd v Australian Competition and Consumer Commission* (2012) 287 ALR 249 at 258 [37], *per* Keane CJ, Finn and Gilmour JJ.
100 *Australian Competition and Consumer Commission v Woolworths Limited* [2016] FCA 44 at [126]. See also *Australian Competition and Consumer Commission v Chrisco Hampers Australia Ltd [No 2]* [2016] FCA 144 at [28]; *Australian Competition and Consumer Commission v ABG Pages Pty Ltd* [2018] FCA 764 at [136]. See further the recent amendments to the statutory ceilings, discussed at n 89.
101 Data Protection Act 2018 s 155(3)(b).
102 Ibid s 155(3)(d).
103 Ibid s 155(3)(f).
104 Ibid s 155(3)(k).
105 Supra (Digital Platforms Inquiry) n 1 at 376–377.
106 J M Paterson and E Bant, 'Intuitive Synthesis and Fidelity to Purpose? Judicial Interpretation of the Discretionary Power to Award Civil Penalties under the Australian Consumer Law' in P Vines and M Scott Donald (eds), *Statutory Interpretation in Private Law* (Federation Press, 2019) 174.
107 Supra n 14 at [137]–[138].
108 Around 6.3 million users in Australia alone created a new Google account on Android mobile devices between January 2017 and August 2019: ibid at [23]. Each of these users was potentially exposed to Google's misleading conduct.
109 D J Solove and D K Citron, 'Risk and Anxiety: A Theory of Data Breach Harms' (2018) 96(4) Texas Law Review 737. See also L Scholz, 'Privacy Remedies' (2019) 94(2) Indiana Law Journal 653.
110 Supra (Digital Platforms Inquiry) n 1.
111 *Australian Competition and Consumer Commission v Australian and New Zealand Banking Group Limited* (2016) 118 FCA 1516 [87], *per* Wigney J.
112 *Australian Competition and Consumer Commission v Reckitt Benckiser (Australia) Pty Ltd* (2016) 340 ALR 25 at 55 [128], *per* Jagot, Yates and Bromwich JJ.
113 Supra n 14 at [65]–[76].
114 R Nakashima, 'AP Exclusive: Google Tracks Your Movements, Like It Or Not' (14 August 2018) *Associated Press* <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> last accessed 1 July 2021.
115 Supra n 14 at [71]–[74]. However, prior to the Associated Press article some employees were at least aware that the 'Location History' and 'Web & App Activity' settings were 'confusing'. See *supra* n 14 at [69]–[70].
116 Ibid at [72].
117 The speed and effectiveness with which the problem was addressed may, however, be relevant factors as evidence of corporate responsiveness: see, eg, French's discussion of the 'principle of responsive adjustment': the capacity to review and adjust the processes to ensure they are performing in the way that is required and expected: P A French, *Collective and Corporate Responsibility* (Columbia University Press, 1984) 164–169. See further B Fisse, 'Reconstructing Corporate Criminal Law: Deterrence, Retribution, Fault, and Sanctions' (1983) 56(6) Southern California Law Review 1141.
118 Examples include deceit, fraudulent misrepresentation, injurious falsehood, knowing receipt and assistance, and unconscionability. See eg, for deceit, the requirement that the defendant knowingly or recklessly misled the victim, intending to induce the victim's reliance: *Magill v Magill* (2006) 226 CLR 551.
119 For example, through remoteness rules and apportionment provisions.
120 Such as good faith change of position, or honest and reasonable mistake.
121 See generally E Bant, 'Culpable Corporate Minds' (2021) 48(2) University of Western Australia Law Review 352; E Bant and J M Paterson, 'Systems of Misconduct: Corporate Culpability and Statutory Unconscionability' (2021) 15 Journal of Equity 63; Australian Law Reform Commission, Parliament of Australia, *Corporate Criminal Responsibility* (Final Report No 136, April 2020) at [6.38].
122 *Lennard's Carrying Co v Asiatic Petroleum Co Ltd* [1915] AC 705 at 713, *per* Viscount Haldane LC; *HL Boulton (Engineering) Co Ltd v TJ Graham and Sons Ltd* [1957] 1 QB 159 at 172, *per* Lord Denning; *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153 at 170, *per* Lord Reid.
123 [1995] 2 AC 500.
124 Eg in Australia *Director of Public Prosecutions Reference No 1 of 1996* [1998] 3 VR 352 at 355; in New Zealand *Jin v Knox Property Investment Limited* [2016] NZCA 565 at [26]; in Singapore *Ho Kang Peng v Scintronix Corp Ltd* [2014] 3 SLR 329 at [47]–[50]. English courts appear to have abandoned the approach: see Law Commission, *Corporate Criminal Liability: A discussion paper* (Discussion Paper, 9 June 2021) at [2.48]–[2.56].
125 *Meridian Global Funds Management Asia Ltd v The Securities Commission Co* [1995] 2 AC 500 at 91, *per* Lord Hoffman.
126 For a detailed critique of this approach, see R Leow, 'Equity's Attribution Rules' (2021) 15 Journal of Equity (forthcoming). See also R Leow, *Corporate Attribution in Private Law* (Hart Publishing, 2022) 35.
127 See, eg, Competition and Consumer Act 2010 (Cth) s 84. The significant exception in Australia is found in its unique 'corporate culture' provisions, contained in pt 2.5 of the Criminal Code Act (Cth) 1995, as to which see supra (Bant) n 121 at 369–374.
128 See, eg, Corporate Manslaughter and Corporate Homicide Act 2007 s 1(3).
129 Supra (Bant and Paterson) n 121. Principles of 'aggregation' that seek to combine the knowledge of individual employees to produce a collective corporate mind have been treated with considerable caution: see, eg, *Commonwealth Bank of Australia v Kojic* (2016) 249 FCR 421 at 449 [112], *per* Edelman J, with whom Allsop J generally agreed at [31], but see also 438 [66], *per* Allsop P and [81]–[84], *per* Besanko J.
130 Supra n 117 (Fisse) at 1189.
131 Penal Code Review Committee, Singapore Government, *Penal Code Review Committee Report* (Report, August 2018) at 212 [10], citing R Mays, 'Towards Corporate Fault as the Basis of Criminal Liability of Corporations' (1998) 2(2) Mountbatten Journal of Legal Studies 31 at 40. See also B Fisse and J Braithwaite, *Corporations, Crime and Accountability* (Cambridge University Press, 1993) at ch 2.
132 See, eg, M Hilb, 'Toward Artificial Governance? The Role of Artificial Intelligence in Shaping the Future of Corporate Governance' (2020) 24(4) Journal of Management and Governance 851; D Wellers, T Elliott and M Noga, '8 Ways

Machine Learning is Improving Companies' Work Processes' (2017) Harvard Business Review <https://hbr.org/2017/05/8-ways-machine-learning-is-improving-companies-work-processes> last accessed 1 July 2021.

133 Supra n 14 at [65]–[74].

134 This approach draws on, among other sources, the 'corporate culture' provisions found in Australia's Federal Criminal Code, which stipulate that a corporation's state of mind may be found in its corporate culture, defined as 'an attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities takes place': Criminal Code Act 1995 (Cth) s 12.3(6).

135 *PT Ltd v Spuds Surf Chatswood Pty Ltd* [2013] NSWCA 446 at [110], *per* Sackville AJA, McColl and Leeming JJA agreeing.

136 *Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) (No 3)* (2020) 275 FCR 57 at 122–123. [386]–[391], *per* Beach J, discussing unconscionable 'systems of conduct and patterns of behaviour' under section 21 of the ACL.