GDPR: Governance Implications for Regimes outside the EU

Coral Ingley
Management Department
Faculty of Business and Law
AUT University
Private Bag 92006
Auckland 1142
coral.ingley@gmail.com

***Philippa Wells**
Federation Business School
Federation University Australia
Victoria, Australia
Ph +61353279653
p.wells@federation.edu.au

Around 120 nations protect personal data with at least another 30 in train. Many regimes reflect the OECD Privacy Guidelines. However, these guidelines, and their regimes, may no longer be effective. The EU's 2016 General Data Protection Regulation (GDPR) is a game changer. That new regulation elsewhere reflects the GDPR suggests much about the impact of globalisation. Inevitably, this impacts organisations in international commerce/business relationships. Three questions are explored with reference to two non-EU regimes: how is the GDPR likely to affect governance of organisations? What gaps are there in existing privacy regimes? And what are the governance and risk management implications?

INTRODUCTION

One of the major "scandals" to hit the world press in 2017 was the association of Facebook with Cambridge Analytica; an association that enabled Cambridge Analytica to harvest and use the personal data of Facebook members. Critics claimed that this data was then used to manipulate the democratic process, including the 2016 U.S. Presidential election (e.g. Meyer, 2018). The widespread negative press around this association claimed its major scalp with Cambridge Analytica filing for Chapter 7 Bankruptcy in New York and its British parent SCL elections Ltd shutting down operations (Reuters, 2018).

From this one example, it is apparent that the protection, control and use of personal data is a major and expanding concern for many jurisdictions. Further, as the capacity of technology increases, and the controllers of that technology expand in size, sophistication and wealth, so too does the potential for (mis)use of data. Lawmakers have not exactly instilled confidence in their ability to control this phenomenon but, instead, "the political class has reacted to the rise of the tech behemoths with the gawping stupefaction of a five-year-old strapped into the nose cone of a space rocket" (Rawnsley, 2018).

One region where lawmakers have reacted is the European Union (EU), most recently via the General Data Protection Regulation or GDPR. This measure, in turn, poses risk management issues (and therefore governance challenges) for a range of organisations, particularly companies, whether large or small, operating either directly in the EU, or indirectly via organisations operating there. These risks and challenges arise not only because of the potentially significant cost of compliance but also the cost of legal proceedings and/or the damage to organisational reputation. With the central imperative of the GDPR (formulated prior to the Facebook-Cambridge Analytica debacle) being the protection of individual data, it

is beyond credible to suggest that it merely represents business as usual for those organisations. There is also the matter of how the GDPR affects, or could affect, strategic decision making by organisations. Already some organisations have announced their intention to abandon operations in the EU due to the GDPR and others are changing their policy and processes to minimise the risks. However, current indications are that not all appreciate the potential risk they face. The Information Systems Audit and Control Association (ISACA) found that fewer than one third of senior executives and boards of directors globally are satisfied with their organisation's progress in preparing for GDPR and 35% of respondents were unaware as to whether their organisation had made any progress at all (ISACA 2018). Closer to this paper's context, it has been reported that almost 10% of New Zealand respondents to the Global Cyber Risk Perception Survey (2018) were unsure whether their activities were subject to any overseas regulation, let alone the GDPR, and 25% of those who did know they were exposed to the GDPR had not developed a data breach response plan (Boles, 2018). However, it is highly risky for those entities that are faced with the reality of the GDPR to ignore and hope. As Durbin (Managing Director of the Information Security Forum (IFS)), puts it, "you never know when a breach is going to take place" (Olavsrud, 2018). Proactive strategies (or organisational resilience) and a culture of compliance is fundamental to the management of risks emerging from this initiative.

Given the above, it appears that organisations are likely to face significant issues and challenges in relation to their governance as per the GDPR with at least some being poorly prepared to address them. It is also important to emphasise that the GDPR is merely one manifestation of the growth of risks, uncertainties and challenges that affect the present and future of different sizes and types of organisation. Thissuggests that research into organisational strategy in this context requires an exploration not just of management of the impact of the GDPR as (yet another) specific and discrete risk (which tends to be reactive and short-term), but also evaluation of responses to its requirements from the perspective of organisational resilience. This evaluation involves addressing the question of "what can… [be done] to ensure the future success of…[organisations] against the growing array of risks?" (a long term, proactive approach) (Hopkin, 2014, p. 252). Although beyond the primary focus of this paper, using organisational resilience as a conceptual framework is appropriate for future research on the governance impact of the GDPR. By way of brief explanation, the approach involves the organisation completing five steps: mapping and identifying (the risk radar), identifying and constructing structures and institutions that can be used as protection against such risks (resources and assets), identifying and mapping impacts from contractual and other arrangements with third parties (relationships or networks), identifying, stress testing and implementation of processes and procedures to minimise likelihood of breach and any negative consequences (rapid response) and, finally, on-going review and appraisal of this process (review and adaption).

By way of historical context to the matter of the protection of privacy of personal data, the Organisation of Economic Cooperation and development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (TBFD) (Privacy Guidelines) (originally promulgated in 1980 and most recently updated in 2013), incorporates 13 principles addressing the collection, storage and use of personal data. Many jurisdictions, both national and subnational, have adopted these principles either as is, or with some modification, with some 120 nations having privacy regimes in place as of 2017. These principles acknowledged the impact on privacy from ineffectively controlled expansion in the use and capability of technology in collection, application, manipulation and storage of personal data and on the transborder data flow issues arising from inconsistencies in national regimes (Kirby, 2010).

In the instance of the EU, The Grand Chamber of the Court of Justice of the European Union has for some years been developing a reputation "for its more purposive and expansive interpretation and application of EU data protection law" (Kuner, et al., 2018, p. 1), most specifically in relation to the EU Charter of Fundamental Rights (2009). The latest development has been the GDPR which, as from 25 May 2018, is fully in force. It is not limited to the private sector, although the focus of much of the publicity and warnings available on the impact of the GDPR has been on its consequences for companies (a tiny cross-section of official, general and sector-specific examples being Brandom, 2018; GDPR Org (nd); Irwin 2017; Kharpal, 2018; New Zealand Trade and Enterprise 2017; OAIC, 2018; Strand, 2017).

The following section provides an overview of the central provisions of the GDPR. This is followed by a similar overview of the privacy regimes in place in New Zealand and Australia (Commonwealth (Federal) only, as under the Australian Constitution, the power to manage external relations is within the Commonwealth ambit (one of its so-called "exclusive" powers). The discussion focuses on similarities and variations between these regimes, particularly those relevant to the activities of "foreign" or external entities where those activities may affect the privacy of protected individuals. This discussion provides a framework in which to explore governance implications for Australian and New Zealand domiciled companies that engage in some way with EU residents or those seeking to do so at some point. It also is worth emphasising that while the GDPR applies only to EU individual data, other jurisdictions are moving to implement similar regimes. Thus, in the longer term, the GDPR provisions are likely to have broad governance implications for all businesses involved in trade with a range of nations and jurisdictions.

THE GDPR

Very briefly (given that it stretches to some 260 pages), the Regulation provides for the protection of personal data of residents ("data subjects") of the EU, whether a threat to the protection of such data emanates from organisations ("controllers or users") in or outside the EU and whether it is direct (arising from a relationship between the individual and an entity possessing or using that data), or indirect (as a result of a third party entity gaining access to that data via the controller or user). More specific and relevant details of the GDPR are as follows (drawing from the useful summary created in 2018 by the Australian Commonwealth Office of the Information Commissioner (OAIC):

- Coverage extends to activities (including supply and transaction-related activities such as payment arrangements) that relate to the offering of goods or services to EU "data subjects" or that monitor their behaviour.
- "Personal data" is (any information relating to an identified or identifiable individual, including any one combined with other data that allows identification of individuals). Thus, details of race cross-tabulated with genetic data may facilitate identification of individuals falling into that specific category. "Processing", the critical activity triggering obligations under the Regulation, means any operation(s) that interrogate(s) personal data whether that operation be automated or not and whether it occurs in the EU or elsewhere.
- Compliance responsibility lies with both the "controller" (the entity that determines the use or means of processing data) and the processor (the one doing the processing as defined).
- Criteria against which any activity is judged for (non)compliance are identified in Article 6(1)(a) and include any, some, or all of: clear consent (by the subject), contextual necessity (e.g. for a contract), necessity affecting the controller (e.g. compliance with a legal requirement), protection (of a vital interest of the subject's), public interest or official authority (e.g. law enforcement or national security) and/or legitimate interests of the controller that outweigh those of the subject.
- Management and regulation of international (transborder) data transfers are specifically addressed. Countries outside the EU may be "white-listed", which means the European Data Protection Board (via an adequacy decision pursuant to Article 45), deems them to have adequate data-protection safeguards such that data can be transferred there without the need for recipients to demonstrate specific safeguards. Only a few countries are presently white-listed. Absent such a status, the controller (located in the recipient jurisdiction) must demonstrate that it has adequate safeguards in place, such as approved codes of conduct or as party to an agreement to comply with the "standard data protection clauses" promulgated by the EU Commission.

- Significant penalties are provided for breach, most particularly those relating to consent, rights of subjects and transborder data flow, these being up to €20 million or 4% of worldwide turnover, whichever is the greater.

NEW ZEALAND AND AUSTRALIAN PRIVACY REGIMES COMPARED TO THE GDPR

GENERAL INTRODUCTION

Australia and New Zealand (both members of the OECD) moved (relatively) early to ratify the original OECD privacy principles through statute (the Australian Privacy Act 1988 (Commonwealth) Schedule 1 (that since 2014 includes the 13 Australian Privacy Principles (APPs) with their scope and exceptions incorporated within each one), and the New Zealand Privacy Act 1993 (s6) (with 12 Information Privacy Principles or IPPs)). However, while the New Zealand statute applied from the outset to the private sector (the first such legislation outside the EU to do so), the Australian legislation originally applied only to the public sector (Blair, 1999). As of May 2018, the New Zealand Act covers "agencies": any person or persons, whether private or public, incorporated or not, while the Australian federal legislation is limited in scope to "APP entities" (s6) – a term that impacts the extent to which the privacy principles apply. Specifically, the term embraces government "agencies", private and non-profit "organisations" (defined as any with turnover exceeding AU $3 million) (s6C – last amended in 2012), private health providers, and some small business operators (subject to limitations) (s6D – last amended in 2012).

The New Zealand legislation has most recently been amended in 2013 and is currently undergoing reform through the 2018 privacy bill. This bill is a response to a series of recommendations in favour of updated legislation (e.g., the Law Commission in 2011 and more recently, the New Zealand Privacy Commissioner who argued that the New Zealand provisions have "fallen …behind international standards" (Edwards, 2017), needing further reform to ensure currency and consistency with trading partners). At the time of writing, this bill is trudging through the parliamentary process (McManus, 2018). *Inter alia*, if passed in its present form, the new legislation will provide for stronger investigation and enforcement powers for the Privacy Commissioner, mandatory reporting of breaches by affected agencies and the issuing of enforceable compliance notices.

The Australian Act was reformed reasonably extensively in 2014 and further in 2017 (to require mandatory reporting by APPs of data breaches). However, the latest narrow interpretation of "personal information" framed by the Federal Court in Privacy Commissioner v Telstra [2017] FCAFC 4 (as information about an individual rather than that which could reasonably be used to identify, based on the previous definition, not the latest under the reforms of 2014), has left the position uncertain (Johnston, 2017). This particularly impacts on the control and use of metadata and data matching programs.

Below is a brief comparison of selected aspects of the New Zealand and Australian regimes that differ from the GDPR, particularly those important to the matter of corporate governance. As part of this discussion, governance implications of the GDPR are identified.

ENTITIES INCLUDED

As identified above, the different privacy regimes are somewhat inconsistent in terms of their entity coverage. In all three instances large corporates are explicitly included in their coverage. It is arguable that such organisations are the most likely to be involved in international trade or data-relevant activities in or connected to the EU and therefore should be most concerned with compliance with the GDPR. However, other types of organisation cannot be complacent.

First, in the global economy, it is likely that goods and/or services will or could be offered to those in the EU, even from as far distant as Australia or New Zealand (e.g. Lundstedt, 2018). Second, in a networked world, even where data may be controlled in the EU, processing can happen at remote locations, including Australia and New Zealand.

To explain: entities/agencies not subject to a privacy regime in their home jurisdiction may have less appreciation of privacy obligations under the GDPR than those who are already required to comply with such a regime. The broad encompassing scope of the GDPR means that not only large corporates but smaller entities face governance issues associated with the Regulation – a matter of concern particularly to those smaller businesses or those without previous or extensive experience with personal data management. Further, frequent media reports of cyber-attacks and data security reveal that even large organisations are vulnerable to hacking and other invasions with consequences for customers (including financial fraud, identity theft, violence and other physical harm (OAIC, 2018)), and for the organisation (including loss of trust, reputation and financial loss). The GDPR data protection requirements and prescribed penalty regime merely serve to indicate how serious are these repercussions and protection implications, to the point that those who may potentially come under scrutiny must implement compliance and management programs to protect themselves against breach, or to minimise the impact should a breach occur.

Additional to this is the requirement in the GDPR (Art. 38(3)) that there should be a Data Protection Officer (DPO) in any controller or processor. Further, this officer must exercise their functions independently and "directly report to the highest management level" (sic). Although it would appear organisations have discretion in how this is to be achieved (Stenz and Taieb, 2018), it could challenge existing expectations and governance/power/management structures and relationships. Given that a fundamental tenet of an agency-driven governance ethos is clear separation of the governance (board) function from management, the question might then be – what is, or should be, the DPO's relationship to management and the board, given that privacy management has strategic, compliance and operational aspects? The lineal relationships are further obscured by the recommendation that the DPO role sit within a risk, compliance, or governance function independent of management or operations and with direct access to the board (Calder, 2017).

TRANSBORDER DATA FLOWS

First, the GDPR, as indicated above, extends to any controller or processor (any natural or legal person, public authority, agency or other body (Art 4)) whose activities involve the "processing of personal data" (defined (art 4) as any…relating to an identified or identifiable natural person"). This coverage is not limited to those located in the EU or even those connected to those in the EU. It suffices if their activities in some way relate to personal data collection, management or use where such activities impact EU residents. As also indicated above, the European Data Protection Board has the authority to "white-list" specific countries outside the EU for the purposes of receiving EU individual data. As at the beginning of 2018, New Zealand is on the "approved" list, but Australia is not.

The New Zealand Act presently addresses the privacy concerns associated with transborder data flows through the Privacy (Cross-border Information) Amendment Act 2010. Under this Act the Commissioner "may" prohibit the transfer of personal information from New Zealand to another state if satisfied on reasonable grounds that "the information [comes]…from another State and is likely to be transferred to another [third State]…where it will not be subject to a law providing comparable safeguards (s114B(1)(a)) and the transfer would be likely to lead to a contravention of the basic principles of national application set out in…the OECD Guidelines" (s114A(1)(b)). This provision has a proactive focus in that the Commissioner is expected to act prior to the transfer of the information: equally, to forestall any complaints, the agency seeking clearance to transfer the information would need to formulate a rationale and justification prior to asking the Commissioner for a ruling (otherwise, surely the Commissioner would need to be prescient?). However, it would appear this process is not mandatory, meaning that those transferring data may elect not to involve the Commissioner at all. Also noteworthy is that the provision not only specifically charges the Commissioner to consider OECD guidelines but also the "European Union Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on

the Free Movement of Such Data" (which the GDPR replaces) (s114A(2)(c)(ii)), thereby acknowledging the importance, relevance and application of legal regimes external to New Zealand. The 2018 bill provides further powers for the Privacy Commissioner in this context in the form of stronger protection.

By way of contrast, the Australian APP 8.1/8.2 and s16C (incorporated into the Act in 2012) embody a reactive approach to this matter, leaving it to the entity to make the pre-transfer determination and involving the Commissioner only if, and when, a breach does occur. Principle 8.1 requires the entity to take "reasonable steps" to ensure the overseas recipient does not breach the Australian APP or, *inter alia*, that the recipient is subject to rules "substantially similar" to those of the Australian regime (8.2). S16C shifts liability for such breaches to the APP entity transferor.

As all three regimes allocate responsibility for ensuring the recipient of cross-border data is subject to substantially similar rules as those affecting the transferor, *prima facie*, the differences between the GDPR and the other regimes do not seem significant (except in terms of the size of penalties and perhaps the determination of the enforcement bodies). However, again there is the issue of risk management: where data is transferred by a controller to a processor. In such a situation, it is possible that the controller could lose control of that data or its use. Hence "reasonable steps" (under the New Zealand and Australian regimes) for the transferor would likely require the exercise of control and oversight through appropriate due diligence (affecting the selection of both the proposed transferee and the regime in which they operate), the management of the data (including the security and protection structures transferees have in place) and destruction (of records by the transferee once the data processing has been completed and results returned). Although this process seems operational, the fundamental financial and reputational impacts for the controller that may arise from misuse or mismanagement means that the board should have at least a watching brief over these operations.

This leads to another aspect where variation between the regimes has potential relevance for the governance of affected organisations. This aspect concerns the nature, incorporation and application of codes of conduct and/or compliance. Consideration needs to be given to how codes are incorporated in the regimes of Australia and New Zealand and whether they accord with the expectations and requirements of the GDPR.

CODES OF CONDUCT/COMPLIANCE

The GDPR (Art 40) provides for codes of conduct as a "semi-self-regulating" mechanism (Bird and Bird, 2017). Such codes can cover any or all data privacy aspects relevant to a specific context and must be approved and certified by a "supervisory authority" (Art 55) (defined in Art 51 as an "independent public authority"). Such certification can be revoked by that same authority should the code at any stage be deemed not to satisfy the conditions for accreditation. Importantly, with its central objective of protecting "fundamental rights and freedoms of natural persons and…their right to the protection of personal data" (Art 1(2)), the GDPR has moved beyond a compliance-with-regulation focus to stipulating the need for demonstrable responsibility and accountability on the part of affected entities,). Accordingly, such codes go to the heart of policy and process for affected entities.

The New Zealand and Australian regimes both provide for legally enforceable codes of practice covering specific industries, processes, or classes of information (s46 (New Zealand) and s46U (1) (Australia). Australia has three codes (covering Government Agencies, market research (limited to members of the relevant industry association) and credit reporting). Data-management in the context of health information and medical research are treated separately under ss95 and 95A (OAIC (n.d.)). These become enforceable once registered (ss26A-S). The focus of these codes is broad compliance with the APPs but in some cases, variation from them. In New Zealand, there are presently seven codes covering such areas as health, credit reporting, superannuation and telecommunications (Privacy Commissioner, n.d.) and often modifying the

application or impact of relevant principles for specific purposes or contexts. These codes, too, are deemed enforceable (as regulations) once registered.

The fundamental difference between the GDPR and the New Zealand and Australian approaches in this context are the foci of, and expectations implicit in, these codes. With the GDPR, their approval and certification are dependent on the sponsoring organisation being able to demonstrate compliance with the underlying privacy principles, while controllers and/or processors must accept the responsibility of something going amiss – a proactive approach. This should be compared to the wording of s46 (NZ) that authorises codes which may prescribe "standards that are *more or less* stringent than the standards that are prescribed by any [privacy] principle" (italics added) (although being required to align with the overarching purpose of the legislation to "promote and protect individual privacy in general accord with the Recommendation of the [OECD]…."). Essentially, these codes provide a "safe harbour" defence to claims that an agency has breached a given principle (s53). The Australian equivalent does not specifically address whether the codes act in this manner although it is probably implied by Ss 26A and L – that provide that entities must comply with any binding registered code. Such compliance would therefore appear to serve as an absolute (safe harbour) defence.

The governance issues specific to this context revolve around the strength and resilience of relevant codes. If New Zealand or Australian codes are weak compared to the GDPR and/or codes approved under it, presumably the safe harbour or other defence would not apply should they be scrutinised by those responsible for enforcement of the Regulation. Thus, either the codes would require updating to reflect the super-national legal requirements of the GDPR, or that individual organisations dealing in or with the EU, and affected by an inconsistent code, would need to pursue a second compliance process or face the risk of breach. With the board responsible for management and organisational compliance and given the significant implications of breach of the Regulation, this process would be a priority. The final aspect to explore is the personal responsibility of those accountable for governance: that is, the directors. This is the focus of the next section.

DIRECTORS' LIABILITY AND RESPONSIBILITY FOR PRIVACY

Many commentators stress the requirement of a top-down approach to compliance with the GDPR. The Regulation has a much greater focus on compliance than do previous or other privacy regimes and makes data protection a boardroom issue (MinterEllison, 2018). The focus in the New Zealand and Australian regimes is on the responsibility of agencies/ entities and the provisions are couched in such terms. The status quo for most board members involves acceptance of assessment by management or consultants of the level of protection needed.

By way of contrast, the GDPR requires that boards become active drivers of better data protection processes. This echoes the theme of a recent article in the Harvard Law School Forum on Corporate Governance and Financial Regulation that the board itself creates a board committee focused on cyber risk and cybersecurity that covers the gamut of potential threats from both internal and external parties. The article makes it clear that directors need to deal in specifics, rather than take an "overview" approach (Diligent, 2017).

Reported research findings reveal some of the implications of this provision on current management and governance processes, most particularly by exposing the shortcomings in board expertise and focus on such matters. In 2015, a survey conducted by the NYSE in partnership with Veracode found that only 4% of respondent directors of companies on the Exchange were "very confident…that your companies are properly protected against cyberattack" (2015, p. 3) with another 29% "confident". Accenture4 found that only 6% of the directors at the world's largest financial institutions have technical expertise (Diligent, 2017). However, according to the 2018 Corporate Board Member/Spencer Stuart "What Directors Think" survey, 67% of participant directors reported their boards bring in experts to help master contentious cyber

issues with another 20% considering doing so in the near future. This reflects the fact that while cybersecurity expertise has not been a core strength sought in candidates for most director positions (the vast majority of directors having finance, legal and business backgrounds), it is more likely now to be identified as a significant issue for boards.

Under the GDPR, the board is accountable for protecting data (Diligent, 2017). Thus, board members must now become active participants in certifying data protection, ensuring cyber-security and being the drivers of internal processes and actions to protect private information. Additionally, directors themselves will have to be conscious of how, when and where they store any board-related documents or communications that contain EU citizen data. Outside directors are included and there is almost no way to absolve individual board members from responsibility. Consequently, board accountability and data protection should be included in the corporate risk register (Calder, 2017) and the matter of Directors and Officers (D&O) liability insurance is of crucial importance (Loopuit, 2016).

THE GDPR AND RESILIENCE IN A PARTICULAR CONTEXT

In 2018, there was a news story (carried in media around the world, including the USA (Griffiths, 2018)) that New Zealand had legislated (via the Customs and Excise Act 2018) to provide for a fine of up to NZ$5000 to be levied for anyone who refused to surrender their on-line/social media access details to immigration officials. Those digging further into this story discovered others also that had similar (or harsher) penalties or implications for such refusal. Although border staff are already empowered to make such demands, Australia is about to introduce a law carrying a potential prison term of up to 10 years for refusal to deliver these details (Njui, 2018). On its ESTA (Electronic System for Travel Authorization) form, the United States now "requests" details of applicants' social media accounts as part of its "extreme vetting" approach to national security concerns (U.S. Customs and Border Protection, 2018; CBC, 2018), and Canadian border officials can demand to see devices on peril of the traveller being denied entry (Kohut, 2017). In the EU, governments have, or are, introducing laws to allow searches of devices held by asylum seekers (Meaker, 2018).

So how is this relevant to the matter of resilience and governance implications in relation to the GDPR? Superficially little, but from another perspective, the implications for organisations, particularly those external to Europe, could be significant. Thus, the issues for organisational resilience could also be significant. The implications emerge mainly from the fact that it is not only the details of the carrier that are available to border officials but also those of contacts, group members and contacts of contacts – the infection effect.

Exploring this matter from the perspective of organisational resilience suggests steps that organisations would be advised to take as precautions. Each of these are discussed with reference to five steps of a risk management strategy as devised by Hopkin (2014).

1. RISK RADAR

The regulation extends its effect outside the EU by dint of the fact it applies to any action by any organisation that directly or indirectly affects the rights to privacy of any EU resident (in the context of products provision or monitoring of behaviour). The GDPR (Art 23) provides that law enforcement activities are exempted from the full gamut of privacy protection provisions but, seemingly, only in the context of certain investigations and not, apparently, in the case of fishing expeditions (although the GDPR does permit jurisdictions to provide specifically for profiling if justified for law enforcement or national security (Arts 22-23)).

Consequently, it is at least conceivable that individual data held on a device scrutinised at any border will be subject to the GDPR where that data is of an EU resident. For example, in this interconnected world, client contact details could be shared amongst those within or across organisation-level collaborative

networks including those details on clients within the EU. Therefore, those details would be available to a border organisation and in some cases, could pass beyond the control of either the organisation or the carrier by being downloaded and stored by the border organisation (e.g. U.S. Customs and Border Protection).

2. RESOURCES AND ASSETS

The GDPR expects organisations to have in place appropriate mechanisms and processes to protect personal data against misuse or wrongful access (as defined). In the instance of large organisations, there should be a Data Protection Officer with direct access to the Board or its equivalent. It is also expected that organisations ensure they are conversant with the provisions lest they leave themselves exposed to significant penalties. Consequently, organisations (data controllers and data processors alike) that enable (not necessarily even authorise) sensitive personal information to be held on an employee's or officer's device that might then be accessed at a border, must take care to ensure this information is not subject to scrutiny in breach of the GDPR, even where that scrutiny takes place in a third country. This requires that affected organisations determine when where and how such information is likely to be accessed and/or downloaded and/or stored and processed by border or equivalent authorities – a difficult ask if reliance is placed on those authorities to provide guidance, particularly when this can change overnight. Anecdotal stories, media reports and personal experiences are likely the only means available to most. What is important is that adequate expertise is available to the Board of the organisation such that the directors can understand and control the collection, management and processing of data as appropriate to address this particular risk.

3. RELATIONSHIPS OR NETWORKS

In this interconnected world, organisations are more likely than not to have international networks or relationships. In the context of private information extracted from devices at borders, we could extend that through 3 or more degrees of separation: Hence a controller who sends data to a processor whose employee then stores the information can face potential liability for misuse or mis-location. Although the GDPR provides for a "whitelisting" process to govern and regulate TBDF, personal whim or negligence is less reliable or predictable. Organisations must therefore be careful of their relationships and networks in order to ensure the control and protection mechanisms of recipients of data are rigorous (including safeguards against hacking); an imperative that increases the burdens of both cost and compliance.

4. RAPID RESPONSE

This addresses remediation, or processes and strategies to deal with the fallout from a breach of the GDPR. Compensation or amendment to the content of data may be appropriate but assumes that the organisation and individual enabling the accessing of the personal data of an EU resident provides the advice of this to the affected individual(s). It may be resilient to keep silent but if, and when, the story emerges (as they are wont to do) the level of betrayal and distrust in the organisation, particularly on the part of vulnerable people, can be significant (as per the Facebook/Cambridge Analytics example). Strong policies and articulated values in the organisation that specifically address these matters are necessary.

5. REVIEW AND ADAPT

This step closes the cycle and charges organisations in the context of the GDPR with keeping a constant weather eye on what is happening in terms of its protection of personal data and the impact of breach of the rules on its own reputation. Hence, insofar as access to data by border authorities is concerned, for an organisation to maintain a reputation, it is important that it seek to improve its processes and practices – and to make that known. The potential problem lies in awareness of this: the adage of "if you have nothing

to fear you have nothing to hide" also raises the possibility that organisations providing for tighter controls over management of third party data may fall under suspicion themselves.

CONCLUSION AND DIRECTIONS FOR EMPIRICAL RESEARCH

Overall, the GDPR has potentially significant implications for governance structures, board composition and many other aspects relating to board responsibility, accountability and transparency, some of which are yet to emerge from this far-reaching regulation. The paper set out to address three questions: first, how is the GDPR likely to affect and influence governance of organisations, not only those domiciled in the EU, but also those trading with it or having a presence there? Second, compared to the GDPR, what gaps are there in other existing privacy regimes and, third, what are the implications for the governance of organisations and their risk management strategies? The regimes in place for New Zealand and Australia were selected as a focus for the exploration of similarities and variations between the GDPR and other regimes. While noting that other jurisdictions outside the EU are moving to implement similar regimes, and regarding the first question, the discussion has provided a framework for identifying governance implications for companies engaged in some way with EU residents, or who are seeking to do so. The key understanding is that the GDPR provisions are likely to have broad and far-reaching governance implications for all businesses involved in international trade, whether or not their own country's data privacy regime aligns with that of the GDPR.

In respect of the second question, the existing data privacy protection regulatory regimes of New Zealand and Australia are somewhat adequate, although the fact that the New Zealand regulation is defined broadly, applied widely and enforced for all types of organisations, makes it thus more closely aligned with the GDPR than is that of Australia, which is narrower in its definition and application and less stringently enforced.

Where there are gaps and discrepancies in such regulations as compared to those of the GDPR, companies trading with the EU (and other organisations dealing in some way with its residents) may need to ensure compliance with both sets of regulations. This may be the best approach towards the management of transborder personal data flows by affected organisations in both New Zealand and Australia.

Insofar as the third question is concerned, we note that, so far, little attention has been paid in the literature to the implications of the GDPR for corporate governance and risk management strategies of affected organisations. Given the move by jurisdictions beyond the EU borders to adopt similar regimes and, given also that the GDPR adds another layer of complexity to the regulatory and other risks facing organisations in an integrated world, a broad-based framework focusing on organisational resilience (Hopkin, 2014) is appropriate for analysing organisational response to GDPR.

With reference to the above, and given the responsibility imposed by the GDPR on the board, research should focus on mapping views of directors as to resources available, and responses and responsiveness of their organisations to the hazards and impacts of the GDPR. It appears from the surveys cited above that directors are less than confident about their understanding of the implications of the GDPR, the current adequacy of their organisational systems for ensuring cybersecurity, and control of personal data collection, storage and use, as well as risk mitigation/prevention of data breaches. Resources are also important, so investigation of board capability regarding the skillsets and IT/cyber expertise would be revealing. With the massive and ongoing emergence of new and increasingly sophisticated web-based technologies, existing commentary has highlighted the need for a much higher standard of board competence and urgent upskilling in this area. Readiness to respond quickly and effectively and to learn from the experience is also important for ensuring resilience. A failure to realise that the GDPR does not mean business as usual also brings risk and, thus, it is important to explore, further, boards' understanding of this risk and its governance implications.

REFERENCES

Bird & Bird (2017). Guide to the General Data Protection Regulation. Retrieved from https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en.

Blair, S. (1999). Privacy Laws and the Private Sector: A New Zealand Perspective, Privacy Commissioner. Retrieved from https://www.privacy.org.nz/news-and-publications/speeches-and-presentations/privacy-laws-and-the-private-sector-a-new-zealand-perspective/.

Boles, F. (2018). Are you ready for GDPR? NZ IoD Directors Brief, Issue 5. Retrieved from https://www.iod.org.nz/Portals/0/Publications/2018_05_Are_you_ready_for_GDPR.pdf.

Brandom, R. (2018). How Europe's new privacy rule is reshaping the internet, *The Verge.* Retrieved from https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice.

Calder, A. (2017). Accountability under the GDPR: What does it mean for Boards & Senior Management? Alan Calder Founder & Executive Chairman IT Governance Ltd 19 January. Retrieved from file:///H:/data/Corporate%20Governance%2023032018/Corporate%20Governance%2023032018/Collaborations%202018/ECMLG/accountability-and-the-gdpr-webinar-jan-19-2016-170322094444.pdf.

CBC (2018, January 18). U.S. border guards can search your phone: here are some details on how, *the Canadian Press.* Retrieved from https://www.cbc.ca/news/technology/usa-border-phones-search-1.4494371.

Diligent (2017). The GDPR Checklist for Directors: Get Ahead of the Cybersecurity Compliance Curve with Four Easy Questions. Retrieved from https://diligent.com/wp-content/uploads/2017/11/WP0032_US_The-GDPR-Checklist-for-Directors.pdf.

Edwards, J. (2017). Need for of Privacy Act Reform is Urgent, Privacy Commissioner, accessed 5 May 2018 at https://www.privacy.org.nz/news-and-publications/statements-media-releases/need-for-privacy-act-reform-is-urgent-privacy-commissioner/.

EGDPR.org (n.d.). GDPR Portal: Site Overview. Retrieved from https://www.eugdpr.org/.

Griffiths, J. (2018, October 3). New Zealand: Hand over phone password at border or face $3,200 fine, *CNN.* Retrieved from https://edition.cnn.com/2018/10/03/asia/new-zealand-customs-passwords-intl/index.html.

Hopkin, P. (2014). Achieving enhanced organisational resilience by improved management of risk: Summary of research into the principles of resilience and the practices of resilient organisations. *Journal of Business Continuity and Emergency Planning*, 8, (3), 252-262.

Irwin, L. (2017, October 16). 10 Steps to GDPR compliance: how prepared are you? *IT Governance*. Retrieved from https://www.itgovernance.eu/blog/en/10-steps-to-gdpr-compliance-how-prepared-are-you.

ISACA (2018). General Data Protection Regulation (GDPR): Securing data, leading with both legal and technical expertise. Retrieved from https://www.isaca.org/About-ISACA/advocacy/Documents/ISACA-GDPR-Position-Paper_mis_Eng_1217.pdf.

Johnston, A. (2017, January 19). Mobiles, metadata and the meaning of "personal information". *Salinger Privacy.* Retrieved from https://www.salingerprivacy.com.au/2017/01/19/federalcourtdecision/.

Kharpal, A. (2018, March 30). Everything you need to know about a new EU data law that could shake up big US tech, *CNBC.* Retrieved from https://www.cnbc.com/2018/03/30/gdpr-everything-you-need-to-know.html.

Kirby, M. (1999). Privacy protection, a new beginning: OECD principles 20 years on. *Privacy Law and Policy Reporter*, 6, (3). Retrieved from http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/41.html.

Kohut, T. (2017, February 27). Canadian border officials can search your cellphone, confiscate your device. *Global News.* Retrieved from https://globalnews.ca/news/3268531/cellphone-search-at-the-border-cbsa/

Loopuit, S. (2016, August 6). GDPR: Five questions every board should be asking. Retrieved from https://minutehack.com/guides/preparing-for-gdpr-five-questions-every-board-should-be-asking.

Lundstedt, J. (2018, March 23). EU's GDPR: what this means to Australian businesses. WP Hosting Retrieved fromhttps://wphosting.com.au/blog/managing-wordpress/gdpr-ndbs-australian-businesses.

MacManus, R. (2018, May 15). Is NZ's new Privacy Bill a match for the EU's GDPR? *Newsroom.* Retrieved from https://www.newsroom.co.nz/2018/05/14/108547/is-nzs-new-privacy-bill-a-match-for-the-eus-gdpr.

Meaker, M. (2018, July 2). Europe is using smartphone data as a weapon to deport refugees. *Wired*. Retrieved from https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations.

Meyer, R. (2018, March 20). The Cambridge Analytica scandal, in 3 paragraphs, what it means for Facebook, for President Trump's world and for every American. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/.

MinterEllison (2018, March 6). Biggest shake up to data privacy laws in 20 years – Are we ready for GDPR?. Retrieved from https://minterellison.co.nz/our-view/the-general-data-protection-regulation-are-we-ready.

New Zealand Privacy Commissioner (n.d). Codes of Practice. Retrieved from https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/.

New Zealand Trade and Enterprise (2017). The Principles of the EU General Data Protection Regulation. Retrieved from https://www.privacy.org.nz/assets/Uploads/EUMR-The-principles-of-the-GDPR-09-2017.pdf.

New York Stock Exchange (2015). A 2015 Survey, Cybersecurity in the Boardroom. Retrieved from https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf.

Njui, J. (2018, October 2). Australia and New Zealand Customs to fine visitors who won't give up phone and laptop passwords. *Ethereum World News.* Retrieved from https://ethereumworldnews.com/australian-and-new-zealand-customs-to-fine-visitors-who-wont-give-up-phone-and-laptop-passwords/.

Office of the Information Commissioner (2018). Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.

_____ (n.d.). Privacy Codes. Retrieved from https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/.

_____(2018). Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response.

Olavsrud, T. (2018, April 10). GDPR is Coming. Are you Ready?. *CIO Magazine.* Retrieved from https://www.cio.com/article/3268002/privacy/gdpr-is-coming-are-you-ready.html.

Rawnsley, A. (2018, March 25). Politicians can't control the digital giants with rules drawn up for the analogue era. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/mar/25/we-cant-control-digital-giants-with-analogue-rules.

Reuters (2018, May 18). Cambridge Analytica files for bankruptcy in U.S. following Facebook debacle. Retrieved from https://www.reuters.com/article/us-cambridge-analytica-bankruptcy/cambridge-analytica-files-for-chapter-7-bankruptcy-idUSKCN1IJ0IS.

Strand, C. (2017). How to Plug holes in Australia's Privacy Laws. CSO Online. Retrieved from https://www.cso.com.au/article/628687/how-plug-holes-australia-privacy-law/.

U.S. Customs and Border Protection (2018). Official ESTA Application. Retrieved from https://esta.cbp.dhs.gov/esta/.

----------(n.d.). Inspection of electronic devices. Retrieved from https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf.