

Section 22

From: Section 22 @governanceinstitute.com.au>
Sent: Wednesday, 3 June 2015 5:23 PM
To: Section 22
Cc:
Subject: RE: Consultation paper on regulatory framework for small proprietary companies
 [SEC=UNCLASSIFIED]
Attachments: Final_letter_personal_information_public_display_officeholders.pdf

Dear Section 22

As promised, here is our letter that we sent to Treasury at the start of the year setting out our concerns with the public display of the personal information of officeholders on the ASIC register. As set out in the letter, we acknowledge that the regulator needs this information, and there must be an address to serve documents if an individual needs to enforce their rights, but the other information need not be displayed (and it need not be a personal address). We also set out our suggestions for a technology-driven solution to this issue.

Section 22

Section 22

further consideration, §Section 22
 Section 22

(where ASIC holds the same information). Our members have decided, upon

Kind regards
 Section 22

Section 22

National Director, Policy & Publishing
 Governance Institute of Australia Ltd

T Section 22
 Section 22

@governanceinstitute.com.au

Level 10, 5 Hunter Street SYDNEY NSW 2000

GPO Box 1594, SYDNEY NSW 2001

W governanceinstitute.com.au



 Section 22

6 January 2015

Diane Brown
Principal Advisor
Corporations & Capital Markets Division
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Diane

Public display of personal information of officeholders

I am writing to express the increasing concerns raised by many of our members in relation to the risk posed to directors and officers as a result of information that can be readily used for identity theft or for assaults on personal security being publicly available on the ASIC register of officeholders. We outline these risks on the following page.

Governance Institute strongly supports the requirement that an officeholder provide personal information to the regulator. This information allows the regulator to take action should the officeholder be in breach of their duties. We also strongly support the public policy that other persons too may need to accurately identify and locate individuals who are officeholders of companies in connection with the protection and enforcement of their personal rights and liabilities.

However, the advent of technology on a global scale has fundamentally altered the capacity to access any personal information held on an individual on a database. How an organisation collects, uses, discloses and otherwise handles personal information is subject to the *Privacy Act 1988* and an organisation must secure the private information it holds. Generally, only authorised personnel are permitted to access the personal details of individuals. While we recognise that the information held on the ASIC register fulfils a different role than that held on other individuals on many other databases, the security of personal information remains relevant.

Current law

The current provisions in the Corporations Act 2001 require public disclosure of personal information about directors and officers of a company registered under the Act. In particular, s 1274(2) of the Corporations Act requires that ASIC must allow certain persons to inspect documents lodged with ASIC. These documents include application for registration of a company and notices containing details of directors and company secretaries. In turn, ss 117 and 205B of the Corporations Act require the following information about directors and company secretaries be disclosed in those documents:

- given names and family names
- all former given names and family names
- date of birth
- place of birth
- residential address.

Accordingly, the ASIC public register displays this personal information about each officeholder.

ASIC does not have the power to exempt persons from, or modify, ss 117 or 205B or the provision in s 1274(2) relating to the right to inspect documents. ASIC is also obliged to keep and maintain such registers in such form as it thinks fit (s 1274(1)) and must consider that the information contained in these registers is mandated under the Corporations Act to be made publicly available.

Section 205D of the Corporations Act is the only basis on which this information can be altered, where officeholders have concerns for personal safety. Under s 205D a person is entitled to have an alternative address substituted for their residential address if:

- their residential address is not on the electoral roll for personal safety reasons, or
- their name is not on an electoral roll and ASIC determines that including their residential address would put at risk their personal safety or the personal safety of members of their family.

Concerns regarding risk of identity theft

Identity theft is feasible if an individual intent on the crime has access to the given and family name, date of birth, residential address and place of birth of another individual. As such, all officeholders on the ASIC public register are at a heightened risk of identity theft.

When associated with identity fraud, identity theft can result in victims experiencing serious negative consequences, including financial loss, inconvenience and in some extreme cases, severe trauma. Governance Institute is of the view that our regulatory framework should not expose our directors and company secretaries to such a risk.

Concerns regarding personal safety

Our concern extends beyond identity theft to the issue of the personal security of senior officers. The companies with which they are involved may provide some level of security to high-profile CEOs and their families, but this is significantly undermined when their residential address is a matter of public record. Furthermore, as interest in the environmental and social impacts of companies continues to increase, a wide range of individuals can become interested in pursuing 'causes' by confronting directors and officers at their homes. For example, recently members of a trade union picketed on the front law of the chair of Aurizon Ltd as they disagreed with a company decision on an industrial relations matter. The picketers noted they had sourced the residential address of the chair from the ASIC public register.

As noted above, in the event of concerns regarding personal safety, it is currently possible for officeholders to obtain a 'silent enrolment' from the Australian Electoral Office which can be used by an officeholder to seek the withholding of publication of their residential address by ASIC, with the address of the company nominated instead on the public register. Of course, in such situations, ASIC retains access to the residential address of the officeholder, which is entirely proper, and information concerning the usual residential address may be disclosed to a court for the purposes of enforcing a judgment debt ordered by the court.

Notwithstanding this, while it is possible for an individual to apply to have their residential address details suppressed on ASIC's public register because of safety concerns, the issue we are raising is one that touches every officeholder whose details are on the ASIC register.

Moreover, any legacy system will hold the information of officeholders whose personal details have been registered over many years and in relation to multiple companies. In a world where electronic information remains traceable and accessible, even if no longer posted, such information remains 'live', available and therefore readily accessible, irrespective of an individual's changed status.

Intersection of public policy with a world changed by technology

Governance Institute is of the view that it is entirely appropriate that ASIC request and retain the personal details of all officeholders on a database subject to strict controls and access.

However, we are also of the view that the open publication of birthdates and birth places of officeholders serves no useful purpose other than for persons with criminal intent. In this world of increasingly faceless transactions, birthdates have unfortunately become by default the first form of identity check by banks, telecommunications companies and other institutions to ascertain that they are communicating with an authorised person. To make readily available the personal information of the business community's most influential officeholders is fraught with risk and a significant magnet for cyber-criminals.

The law requires a director to be 18 years of age. Date of birth is therefore essential to accurately identify if a person consenting to be a director meets the statutory requirement. A date of birth may also be useful in correctly identifying officeholders who share the same name, for example, John Smith. When date of birth is triangulated with place of birth, correct identification is assured.

However, while date of birth and place of birth are necessary to ensure correct identification by the regulator as to one particular officeholder being involved with one company rather than another, neither date of birth nor place of birth are necessary should an individual need to locate an officeholder to enforce rights and obligations if the triangulation has already been undertaken by the regulator. The address is required in this instance.

The issue therefore becomes one of ensuring that the public policy test is met while not putting officeholders at risk of identity theft or infringement of their personal safety.

Recommendations for reform that meet the public policy test

Governance Institute is of the view that technology provides a solution to the accurate identification and location of officeholders should either the regulator seek to take action if the officeholder is in breach of their duties or any individual seek to locate an officeholder in connection with the protection and enforcement of their personal rights and liabilities.

We recommend that a unique ID be introduced by ASIC for each officeholder.

ASIC currently uses a code to suppress the address of a director if they have gone through the Electoral Commission process for a 'silent enrolment's, so some thought has already been given to the use of technology to identify an officeholder.

The assignment of a unique identification code (ID) for each officeholder would:

- ensure that the regulator continued to hold all of the personal information required to correctly identify an officeholder and their connection to any particular company or companies (including legacy information)
- remove the risk of identity theft which is currently posed by the public display of personal information of officeholders, given that identity theft is facilitated greatly by the provision of date of birth, place of birth, full and former names and residential address.

One key business efficiency advantage of unique officeholder IDs that could be explored by ASIC, consistent with ASIC's deregulatory initiatives¹, is that this initiative should allow an officeholder to submit a single change of family name or change of address (residential or

¹ Refer ASIC Report 391, *ASIC's deregulatory initiatives*, May 2014 (Para 1) in which it is stated that ASIC's mandate is to 'strive to reduce business costs and administer the law effectively with a minimum of procedural requirements'.

service address) to their ID data, which could then flow through to update all of the companies of which this person is or was an officeholder. It is highly inefficient for officeholders on multiple companies (especially entities with multiple subsidiaries) to have to lodge this same information over dozens, and sometimes hundreds of companies.

Any individual seeking to locate an officeholder to enforce rights and obligations could locate the officeholder they seek through the use of the officeholder ID. Any search would be conducted by using the name of the officeholder and company. It would be rare for two directors with the same name to serve on the board of one company, although it is possible. For example, currently there are two Mark Johnsons serving on the board of Westpac. However, given that the individual would be seeking to locate all officeholders of the one company, this would not be a concern.

Other parties are also interested in identifying and at times locating particular officeholders, as they seek to assess who has an interest in particular companies. Such third parties include the media, lawyers, banks and other creditors, liquidators and real estate firms. The use of an officeholder ID would assist this, as it would assist any individual seeking to locate an officeholder, as the ID held by the officeholder would reveal all of the companies with which they are involved. There are advantages to linking officeholders in this way, both for the regulator and those seeking to locate individuals in connection with the protection and enforcement of their personal rights and liabilities.

We also support the need for a mechanism to be publicly available in order to serve documents on officeholders. If an officeholder ID is used, there would need to be an obligation on each officeholder to provide a service address. However, the public generally does not need access to the residential address of officeholders.

We recognise that legacy data will probably not be able to be dealt with. Existing records of officeholders' personal information embedded in a vast number of documents filed with ASIC and displayed on the public register will still be available as it would be wholly impractical for such information to be removed. The UK tried to contain the problem when it moved away from the public display of residential addresses by removing data only upon application. We would recommend a similar approach in Australia.

Other jurisdictions

It is of interest to consider the statutory obligations for the public display of personal information of officeholders in other jurisdictions. Assessing whether less personal information is required to be publicly displayed in other jurisdictions, and whether this has any negative impact on the capacity of regulators to take action or officeholders to be located as appropriate, is useful in considering if changes to our statutory framework are feasible.

The detail of requirements in other jurisdictions is set out in Appendix 1, including in a matrix in which all requirements can be easily compared.

It is clear from consideration of other jurisdictions Australian officeholders are far more exposed than their international counterparts in terms of their general right to privacy, personal safety and security.

Scoping study into the sale of the ASIC registry business

The proposed sale of ASIC's registry business highlights further the issues we have raised in this letter. Issues of data control, security and assurance will need to be considered in relation to the sensitive information currently held on the ASIC register.

There could be strong commercial interest in the personal information contained on the register. Information that is compelled by statute in order to ensure that the regulator can take action

should an officeholder be in breach of their duties or to assist individuals in connection with the protection and enforcement of personal rights and liabilities has been provided for reasons of public policy, however, and has not been provided for commercial application. It is important that any such information be collected for regulatory reasons, but it should not be made available publicly for the reasons set out above or for commercial application, as this would be a fundamental breach of privacy and a misuse of the rationale for the public policy.

Conclusion

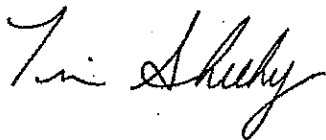
Governance Institute recommends that:

- ASIC retain the personal details of all officeholders
- ASIC issue each officeholder with a unique identification code
- the ASIC public register not display the date of birth, residential address and place of birth of officeholders, but the officeholder name, unique identification code and a service address.

Governance Institute recognises that amendments to the Corporations Act would be required to facilitate these reforms. Governance Institute also recognises that public consultation would need to be undertaken with stakeholders on any such reforms.

We would be more than happy to meet with you to discuss this matter.

Yours sincerely



Tim Sheehy
Chief Executive

T +61 2 9223 5744 F +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

Appendix 1: 2014 Comparison of information obtained by regulators and made available to general public

Table 1: 2014 Comparison of information obtained by regulators and made available to general public

	Information provided to the Companies office				Information shown on the public register					
	Australia	NZ	UK	USA +	Sth Africa	Australia	NZ	UK	USA	Sth Africa
Full name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Former names	✓	-	-	-	-	✓	-	-	-	-
Date of birth	✓	✓	✓	No	✓ or ID	✓	No	✓ *(under review)	No	✓ or ID
Place of birth	✓	✓	Nationality only	No	No	✓	No	Nationality only	No	No
Residential address	✓	✓	✓	No (May show work addresses or PO boxes on forms lodged)	No	✓ @	✓	Can opt for 'service address' in place of residential address on public register #	No (May show work addresses or PO boxes on forms lodged)	No
Occupation			✓							No
Passport ID required for non-citizens					✓					
Officeholder ID code			-Under consideration		Or Passport					

South Africa

- The Companies Act (s 24(5)) requires all companies to maintain a record of directors reflecting full name, date of birth or ID (passport number if not a citizen of the Republic of South Africa). Addresses are not required. This register is open to inspection by securities holders free of charge and any member of the public on payment of a fee (s 26)).
- Companies are required to supply to the regulator [CIPC] the telephone numbers (landline and mobiles) as well as email addresses, when notifying appointments/changes of directors. The regulator has insisted on this to enable them to contact the directors directly when the company's agent notifies changes to the regulator. This is a fraud prevention measure to prevent company 'hijacking'. However, public disclosure by the regulator of its records **excludes** director contact details and conceals certain aspects of director ID numbers to ensure privacy.

United States

The US has a two-tier regulatory model. Securities laws are enforced by the Securities Exchange Commission (SEC) at the federal level and laws governing companies are enforced at an individual state level by state-based regulators.

Officers and directors of public companies in the US are not required to submit their place and date of birth to the SEC, nor are they required to do so under company law in the State of Delaware (where over half of all US companies are incorporated) or any other significant US state jurisdiction.

The only public information about directors and officers is their age and work history, which is contained in the proxy statement (the US version of the notice of meeting). Addresses on other filings, such as under Section 13 of the Securities Exchange Act reporting ownership over five per cent of a company's shares (the US equivalent of Substantial Shareholder Notices), are usually work addresses or PO boxes.

Directors of insurance companies regulated by individual states are required to disclose more detailed information to their state regulators, including their date of birth and other personal information for the purpose of the state vetting them. Similar provisions exist for state bank directors and other highly regulated industries. However, none of this information is made public.