**Supplementary Submission No 3a**

# REVIEW OF THE PUBLIC INTEREST DISCLOSURES ACT 1994


**Organisation:** Office of the Privacy Commissioner New South Wales

**Name:** Dr Elizabeth Coombs

**Position:** NSW Privacy Commissioner



**Date Received:** 21 September 2016

office of the privacy commissioner
new south wales

Mr Lee Evans, MP
Chair of the Committee on the Ombudsman,
The Police Integrity Commission and
The Crime Commission
Parliament of New South Wales
Macquarie Street
Sydney SW 2000

RECEIVED 21/9/2016

19 SEP 2016

Dear Mr Evans Lee,

RE: NSW Privacy Commissioner's submission
Review of the Public Interest Disclosures Act 1994

Thank you for the opportunity to address the Committee.

I recommend that the *Public Interest Disclosures Act 1994* (PID Act) be amended to enable the Privacy Commissioner to receive and deal with public interest disclosures regarding matters that appear to be:

- Conduct contrary to the provisions of privacy legislation, and
- Conduct under the *Data Sharing (Government Sector) Act 2015* and the *State Records Act 1998* that may amount to contraventions of the privacy legislation.

I set out the reasons and evidence for this recommendation.

## The PID Act

The public policy aims of the PID Act are to:

- Enable public officials to make confidential disclosures about the conduct of public agencies or individual public officials who may contravene a number of expectations placed on them.
- Facilitate independent investigation of those disclosures.
- Protect persons who make disclosures from reprisals or other liability for making a disclosure.
- Create a punishments regime for those who take detrimental action against those who make disclosures.
- Render those who take detrimental action potentially liable to pay compensation for any reprisal action.



cc

These measures create a strong framework that enables public officials to bring to the attention of specifically authorised specialist agencies contraventions of standards that public agencies and public officials are expected to observe regarding alleged corrupt conduct, serious maladministration, serious and substantial waste, pecuniary interests contraventions in local government and failures to exercise functions in accordance with any provision of the *Government Information (Public Access) Act 2009* (GIPA Act).

**Statutes that raise the need for privacy protecting measures**

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act), regarding which the Privacy Commissioner has review, oversight, investigation, assistance and educative functions.

One of their aims is to provide enforceable remedies for the protection of the privacy of individuals regarding the life cycle of personal and health information in the functions of public sector agencies, and, in the provision of health services in the private sector.

The two privacy statutes enact obligations regarding personal and health information that are quite unique.

Additionally to the two privacy statutes privacy contraventions may arise from the conduct of public sector agencies under the *State Records Act*. For example, regarding failures to take reasonable measures to protect personal and health information in flows of information between "public offices" and the Authority, storage of that information and decisions regarding what information may become open to the public.

More significantly, the recent enactment of the *Data Sharing Act* regulates flows of information between public sector agencies. Briefly state, the objects of the Data Sharing Act are to:

- Promote the management and use of the valuable resource that is government sector data in a way that recognises the protection of privacy as an integral component, and, provide for compliance with the privacy legislation.

- Remove barriers that impede flows of information between government agencies, and, between government agencies and the Data Analytics Centre.

- Regulate the flows of information by specifying purposes and circumstances of those flows.

- Require compliance with data sharing safeguards.

Sections 11 to 15 discuss the data sharing safeguards regarding privacy interests, other commercial interests and state interests that sharing of information is expected not to violate.

## The Significance of the issue

Data flows between public agencies and from agencies to the community has increased in quantity. Technology makes it easy to trigger a movement of information to many places at once, store it for use at many places and reach a wide audience at once.

Lord Justice Leveson gave an address at the University of Technology, Sydney in 2012 on the topic of Privacy and the Internet. His lordship's comments touched on what the most quoted article on privacy from 1890 identified as an emerging threat. His Lordship said:

> *"The problem which Warren and Brandeis identified was that, as they put it, gossip was no longer the resource of the idle and the vicious. It had become a trade."* ([1])

Although his Lordship's comments were about the press and bloggers, the same could be said about this potential applying to employees of entities that hold personal and health information.

Privacy continues to be undermined by the curious, the malicious and those who design information management systems that fail. Data breaches remain a significant social issue and result in frequently reported regulatory action.

His Lordship addressed the need to have in place a structure to enable genuine whistle blowers to make confidential complaints. ([2])

Whether because of failures of the systems themselves, or, failures of process design, or, human intention to misuse information, we have a capacity to cause greater harm at a simple touch of a keyboard than at previous times.

At times past information storage and management systems did not have the kind of capacity to bring together at the one place as much information about an individual as today's technologies.

Small errors or isolated mischievous conduct has the capacity to reveal far more sensitive information about us.

---

1 Lord Justice Leveson, *Privacy and the Internet*, Communications Law Centre, University of Technology, Sydney, 7 December 2012

2 *An Inquiry into the culture, practices and ethics of the Press*, Report, November 2012, Volume 2, at 994

office of the privacy commissioner
new south wales

## Recent research

Recent research shows that data breaches are on the rise, both in terms of frequency and in terms of the significance of harm they cause. This has been noted in the United States of America, where data suggests that 52% of breaches were most likely the outcome of malicious insiders. ( [3] )

The trend in the United States has continued to the present year. Recent reporting regarding failures to protect consumers' information indicates that regulators have started to impose sanctions in excess of US $2,000,000 and US $5,000,000. ( [4] & [5] & [6] & [7] )

The same trends have been reported in Canada in the areas of civil liability and regulatory action. ( [8] & [9] & [10] & [11] )

The dismissal decision of Nurse McLellan in 2012 described the unlawful accesses to patient information as "mind boggling."

Such conduct that occurred over a period of seven years may well have been avoided, or reduced, if there were in place better processes of auditing or reporting illicit conduct.

The Digital Guardian also has recently reported on the significance of the issue. ( [12] )

The United Kingdom Information Commissioner's trends publications also report high numbers of data breaches. The ICO's publication indicates a concentration of incidents in the health sector and a high probability that human malice has been the cause. ( [13] )

Data breaches are not the outcome of just accidents. Malice or unlawful curiosity affects the conduct of public officials, including the police. Under freedom of information law a non-government organisation obtained numerical information regarding unauthorised handling of information by police in the United Kingdom. ( [14] )

---

3 Covington- Inside Privacy- 30/4/14
4 Department of Human Services- 21/7/16
5 Department of Human Services- 4/8/16
6 Hunton & Williams- 2/8/16
7 Hunton & Williams- 8/8/16
8 Canadian Medical Association- 6/3/12
9 Information & Privacy Commissioner of Ontario- January 2015
10 Western Journal of Legal Studies – Volume 6 - 2015
11 The Star- 29/4/2016
12 The Digital Guardian - 27/6/2016
13 Information Commissioner's Office - 29/4/16
14 Big Brother Watch- July 2016

The statistics for 2,315 incidents for access and disclosure of information from 1 June 2011 to 31 December 2015 merit noting:

1,283 (55%) cases resulted in no formal action being taken.

297 (13%) cases resulted in resignation or dismissal.

70 (13%) cases resulted in conviction or caution.

258 (11%) cases resulted in written or verbal warning.

The Australian Federal Privacy Commissioner has been reported as advising organisations to prepare for more data breaches. ( [15] )

In New South Wales public officials have also been convicted for unlawfully dealing with information.

I am aware of three reported criminal convictions involving police officers and a prosecutions lawyer. ( [16] & [17] & [18] )

I am also aware of a conviction of an Ambulance employee. On 26 June 2015 the Downing Centre Local Court imposed a sentence of 100 hours Community Service for accessing and disclosing the health information of another employee to a private solicitor.

Public employees' convictions are not isolated to NSW. A recent Western Australian Supreme Court decision highlights the fact that in that State also public officials misuse other people's personal information held in government records. ( [19] )

**The offices empowered to receive public interest disclosures under the PID Act**

The Parliament has sought to include as offices empowered to receive and deal with public interest disclosures a number of specialists in the oversight branch of administration. The PID Act empowers each of these offices to deal with matters that fall within their particular field of expertise and as related by their statutory functions.

This does not include alleged contraventions of provisions in the three statutes I mentioned above regarding the handling of personal and health information.

---

15 Sydney Morning Herald- 30/4/2012
16 Salter v The Director of Public Prosecutions (NSW), Court of Appeal – 14/7/2014
17 Hughes v R, Court of Criminal Appeal - 24/2/2014
18 Braimah- Mahamah v R, District Court – 15/7/2016
19 *Cogan v Velkovski*, Western Australian Supreme Court – 9/5/2016

office of the privacy commissioner
new south wales

## Reluctance to make complaints

The making of allegations of contraventions of relevant laws or standards is anxiety generating for many persons. This is more intense for employees, who may fear that putting their name to a complaint about colleagues or supervisors may:

- Harm their prospects of career advancement,
- Result in poor performance reviews, and
- Cause isolating or other retributive conduct by colleagues.

Agency employees contact us to discuss concerns in the following categories:

- Systemic issues that create privacy risks.
- Individual decisions of supervisors that are contrary to the privacy rights of other employees or the community.
- Reports of privacy infringing behaviours that are not properly investigated or addressed.
- Unlawful misuse or disclosure of personal and health information by colleagues.

In our experience these persons tend to avoid disclosing:

- Their name to us,
- The name of the agency where they work, and
- Exact particulars from which we may identify the relevant agency.

My office can therefore be left without sufficient information to take action, or, to make a request for investigation to the relevant agency.

In our experience a common theme in these instances is that informants feel they will not be protected if they complain directly to their employer.

office of the privacy commissioner
new south wales

## Submission

There have always been significant risks of public sector agencies and/or individual employees misusing or disclosing personal and health information. The 1992 ICAC inquiry into the unauthorised of release of personal information clearly established that this occurred and that there is a market for such information. The subsequent introduction of privacy legislation has not eradicated such practices.

The advent of the Data Sharing Act may generate new threats to the privacy rights of the community simply because of the element of 'fadism' that exists around such topical innovations. In the experience of my Office public officials are reluctant to make complaints about privacy related matters directly to their employer, or, to send complaints to my office for investigation for fear of retribution.

A PID Act provision for the Privacy Commissioner is even more appropriate now that algorithms and the Internet-of-Things means that invasion of privacy can occur without a perpetrator per se. In such cases it will be difficult to lodge a complaint for Internal Review by the agency concerned about something that is invisible to daily service users, but which could be known internally by those familiar with the systems and data analytics.

Also, the use of private sector service providers for services that were traditionally delivered by government expands, may increase the risks of improper releases of information to the private sector.

Investigations by the Privacy Commissioner in such cases will be the optimum way to encourage agencies to develop more privacy respecting practices, before any systems or practices deteriorate and create reputational harms and liability risks.

There is a gap in the public interest disclosures legislation in not having a specialist empowered to receive and deal with allegations of systemic privacy undermining practices or intentional privacy contraventions by public sector employees.

Filling the gap by empowering the Privacy Commissioner to receive PID Act disclosures will be consistent with the Parliament's previous decisions to include specialist officials in the scheme, who bring with them their particular experience in the interpretation of the laws that they administer.

We do not have a mandatory data breach notification law in New South Wales. Being able to make public interest disclosures to the Privacy Commissioner will be one way of bringing to attention issues regarding possible mismanagement of personal and health information that may otherwise continue to create risks to the community.

As some of the examples in the annexures show, when risks remain untreated greater damage results in the long run. An amendment to the PID Act will provide for one more safety valve in the system of protections already in place to enable officials who are

prepared report possible mismanagement of information systems feel safer in notifying the appropriate specialist in the oversight branch of administration.

Conclusion

In light of the significant commitments that the Parliament has made for many years to the benefits that the public interest disclosures scheme brings to public administration I consider that updating the scheme in a way that complements policy settings it already contains will support the scheme's operation and enhance the protections of the privacy interests of the community.

I thank the Committee for the opportunity to present this submission.

Yours sincerely

[redacted]

Dr Elizabeth Coombs
NSW Privacy Commissioner
19/9/2016

## Additional machinery provisions that need updating

Section 25 of the PID Act

An office empowered to receive a public interest disclosure may decide to refer the matter to another more appropriate office or to the agency whose conduct may be involved.

This scheme of referrals does not include the possibility to refer a public interest disclosure that specifically alleges contraventions of the privacy legislation or the Data Sharing Act. These fall outside the specialist expertise of the offices empowered to receive public interest disclosures.

Section 6A of the PID Act

Section 6A lists the membership of the Steering Committee established under the PID Act and provides for the Committee's functions.

If the Privacy Commissioner becomes empowered to receive public interest disclosures, membership on the Committee will be necessary, so that the community's privacy rights will have a voice regarding the operation of the PID Act.

Part 3, Division 5 of the GIIC Act

Sections 31 to 35 of the GIIC Act discuss a scheme of permissions for the Information Commissioner to disclose information to the following offices, if the Information Commissioner considers that information relates to the conduct of an agency that could be amendable to investigation under their legislation:

- Ombudsman
- Independent Commissioner Against Corruption
- Director for Public Prosecutions
- Police Integrity Commission

The referrals scheme does not envisage that the Information Commissioner may refer to the Privacy Commissioner information the Information Commissioner received that potentially raises privacy violations.

Section 34 of the GIIC Act enables the Ombudsman to refer a matter to the Information Commissioner, if it could be subject of complaint to the Information Commissioner under the GIIC Act. This discloses an intention that the Information Commissioner is the appropriate specialist to receive and deal with complaints regarding contraventions of the GIPA Act.

This referral arrangement does not deal with the possibility that information received by the Ombudsman may raise issues regarding privacy violations.

It is in the public interest to ameliorate these referral issues, so that the more appropriate specialist oversight agency can be the investigating authority.