Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Salmat Submission to

The House of Representatives Standing Committee on Social Policy and Legal Affairs

July 2012

INTRODUCTION

1. Salmat welcomes the opportunity to make a submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs on the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) (**the Bill**).

2. Salmat is a member of the Australian Direct Marketing Association (ADMA) and supports ADMA"s submission on the Bill.

3. Salmat agrees with the need to reform the privacy regulatory regime in Australia. We support the overall objective of the Bill and the purpose of each of its parts. In particular:

   - The creation of a single set of Australian Privacy Principles
   - The clarification of the function and powers of the Privacy Commissioner (the Commissioner)

4. However, Salmat has practical concerns with certain provisions of the Bill as they are currently drafted and believes that simple amendments to the Bill (suggested below) will provide greater certainty for business, improve compliance, and importantly, create a more effective framework for the increased protection of privacy in Australia.

5. In the age of big data, the amount of personal information that is stored and processed by organisations, both on and off-shore, will continue to grow exponentially. In that context, the focus should not be on individual breaches (which could extend into the millions), but rather ensuring that organisations have the systems, procedures and practices in place to adequately protect privacy.

6. Unfortunately, with human interaction in automated processes, errors sometimes do occur. No regulatory regime can prevent that given the quantity of data that is now being generated.

7. Salmat submits that the core objective of the privacy reforms should be to achieve a principles based regulatory regime that encourages organisations to have the strongest possible systems, processes and procedures in place to protect privacy, while ensuring that the regulatory burden is not so excessive that it threatens the ongoing viability of the business or stifles competition and innovation.

8. We believe that penalties (as opposed to reimbursement for direct loss) are not the appropriate policy response in relation to privacy reform, rather damage to the reputation of data holders is much more likely to have an impact upon compliance and business models.

9. Our contention is that the legislation in its current form does not have the balance right, being unnecessarily and disproportionately punitive for organisations that have adequate systems, processes and procedures in place to protect privacy.

SUMMARY OF CONCERNS

10. Salmat has three main concerns with the Bill:

    I. What constitutes a „serious and repeated interference with privacy" (section 13G) and related issues with associated provisions on penalty regime (sections 52, 80W(6), 80Z)

    II. The unnecessary and confusing prohibition on direct marketing (APP 7)

    III. The need to provide clarity around the collection of personal information when an outsourced service provider is involved (APP 3)

CONSULTATION

11. Since the reform process begun in 2006 with the reference by the then Attorney-General, the Hon Philip Ruddock MP, to the Australian Law Reform Commission, the public has had numerous opportunities to comment on the proposed amendments to the Privacy Act 1988 (the Privacy Act) and associated legislation.

12. Salmat notes that many of the provisions contained in the Bill differ significantly from the Exposure draft that was originally considered by the Senate Finance and Public Administration Committee and have not been subject to a public consultation process as expressly promised by the Government.

13. In particular, Salmat is disappointed that industry was not adequately consulted on the new provisions that deal with the functions and powers of the Commissioner. Many of these provisions have far reaching ramifications for business and should have been afforded the appropriate scrutiny through a public consultation process before the Bill was introduced into Parliament.

ABOUT SALMAT

14. Salmat is Australia"s leading multichannel communications provider. We help our clients communicate with their customers across a broad range of communication channels including voice, mail, online, mobile and social media.

15. Salmat is a market leader in:

- **Business Process Outsourcing** – Australia"s largest provider of transaction essential mail services (bank statement, utility bills etc) with over 1.2 billion mail packs lodged with Australia Post each year.
- **Catalogue delivery** – Australia"s biggest letterbox distribution network delivering over 5 billion catalogues per year.
- **Contact Centres** – Australia"s largest outsourced contact centre provider that has approximately 100 million conversations on behalf of our clients.
- **Digital Communications** – email, sms, social media, mobile, online, e-commerce, data – sending over 600 million emails each year.

16. Salmat is trusted by many of Australia"s iconic brands to look after their data and communicate with their customers. We partner with leading organisation across industries including:

- Banking and financial services
- Government
- Retail
- Utilities
- Transport
- Media services

17. The nature of our customer communication business means that we have deep integration with our clients and their systems. This relates to how they use their data and how they communicate with their customers. Therefore, we deal with billions of records of customer data (often personal information) on a regular basis.

18. Some examples of the type of work that we do for clients are:

- Statements for many of the major banks and financial institutions
- Archiving for the broad range of client across different industries including the banks.
- Government communications including notices of assessment, payments/cheques
- Digitisation of records for government agencies, health insurance companies and hospitals
- Land title, tolling, roads registration details for QLD and VIC
- Outbound telemarketing sales
- Contact centre inbound customer service
- Loyalty programs
- Outboard SMS and email direct marketing
- Speech recognition biometric solutions for identification purposes

19. Salmat takes its obligations under the Privacy Act very seriously and has extensive security and privacy processes in place to ensure that the personal information supplied to us by our clients is protected to the highest standards. This includes comprehensive and regular training of all staff.

20. Salmat has in place company wide compliance to ISO9001:2008 series and more relevantly to the ISO 27001:2006 security series.

21. The proof of the robustness of our systems and processes is that so many of Australia"s leading organisations across many industries trust Salmat to deal with the personal information of their customers.

22. Salmat does not use customer data for any purposes other than at their direction. We jealously guard our reputation as a trusted custodian of customer data and are acutely aware that any misuse would result in significant damage to our reputation.

SALMAT COMMENTS ON THE BILL AND SUGGESTED AMENDMENTS

Section 13G serious and repeated interferences with privacy

24. It is important that the offence provisions apply only in the case of recklessness or intentional disregard for the privacy of an individual. That is, if a company has all the systems, procedures and practices in place to adequately protect the personal information of an individual, then it should not be disproportionately punished when an unintentional error occurs.

25. As mentioned above, Salmat deals with billions of records of personal information on behalf of our clients. Errors have occurred in automated processes which have unfortunately caused multiple breaches of privacy which could have been deemed serious under the new provisions despite Salmat having adequate systems, procedures and practices in place. A recent investigation by the Office of the Australian Information Commissioner confirmed that:

> *"Salmat has reasonable steps in place to protect the personal information it holds from misuse and loss and from unauthorised access, modification and disclosure."*

26. Therefore, we submit that it is essential that the concept of a „serious interference" be clearly defined to create some certainty for business.

27. We note that „serious credit infringement" is defined under section 6 and submit that „serious interference" should also be defined under that section.

Recommendation

28. In Section 6, define "serious interference" as meaning "***reckless or wilful and intentional***"

29. or insert those words in place of the word "serious".

    Reword clause (a) as follows:

    "The entity does an act, or engages in a practice, that ***either recklessly or wilfully and intentionally***, interferes with the privacy of an individual".

SECTION 52 DETERMINATION OF THE COMMISSIONER

Section 52 (1)

30. As currently drafted, the Commissioner may make a declaration as to the steps which must be taken; appropriate redress, compensation etc, without first making a declaration that there has been an interference with privacy.

31. The Commissioner should be **required** to make that declaration that there has been an interference with the privacy of any individual **before** making a declaration about the steps that must be taken.

Recommendation

32. Revise the drafting, so that any declaration must be preceded first by a declaration under (a) (i) and then any of the items following in (b) onwards.

Section 51(1)(iii)

33. An award of financial compensation for an error which affects a large organisation that deals with substantial amounts of data could be disproportionately punitive. We submit that this should be limited only to serious cases and capped.

Recommendation

34. Compensation for loss or damage- add to the end of this clause ***"in circumstances where there is a reckless or intentional interference with the privacy of one or more individuals"***

Section 3A

35. A power to include any order whatsoever is too broad. Such matters are better left to the courts.

Recommendation

36. Delete 3A

Section 80W(6) civil penalty orders

37. As discussed above, Salmat firmly believes that organisations that have adequate systems, procedures and practices in place to protect privacy, should not be disproportionately punished when unintentional errors occur. In that context, we believe that the courts should be required to consider a broader number of matters when determining the pecuniary penalty under section 80W(6).

Recommendation

38. Add the following considerations:
"(e) the nature of the entities business
(f) the systems, procedures and practices the entity has in place
(g) the effect on the industry in which the entity operates.
(h) any other relevant circumstances"

Section 80Z Multiple Contraventions

39. Section 80Z (2) does not make it clear that the maximum penalty is $1,105,000.00 for a corporate entity regardless of how many individuals were affected by the one „breach". Given the vast amounts of data now held by organisations, a single unintentional error can cause multiple breaches of the Privacy Act (in some cases thousands).

40. The current wording seems to imply that if there were, for example, 50 breaches resulting from the same error, then the maximum penalty could be over $50 million. This outcome could cripple a business and is an unnecessarily disproportionate regulatory response.

Recommendation

41. Section 80Z(1) - Change „may" to „must" so it reads:

*"(1) The Federal Court or Federal Magistrates Court **must** make a single civil penalty order against an entity for multiple contraventions of a civil penalty provision..."*

42. Section 80Z(2) - Insert at the end:

"The pecuniary penalty in total must not exceed the maximum pecuniary penalty that could be ordered under sub-section 80W(5)"

APP 7- Prohibition on Direct Marketing

43. Salmat notes that this is the first time a prohibition on direct marketing has been included in the Australian Privacy Principles since the reform process began in 2006. The inclusion of the „prohibition" is confusing for business and consumers because the APP in effect ***permits*** direct marketing under certain circumstances.

    a. Consumers will be confused because APP7 now says that organisations must not use personal information for the purposes of direct marketing with a few exceptions. When consumers continue to receive direct marketing communications (after the Bill receives Royal Assent), they will understandably be confused. This may lead to a significant increase in unmeritorious complaints and is contrary to the intention of the APP which is to ***permit*** direct marketing in certain circumstances.

    b. Businesses and marketers will also be confused with a prohibition on direct marketing with a few exceptions. APP7 is unnecessarily complex and we would assume that marketers would find it difficult to determine when in fact direct marketing is permitted.

44. This confusion is unnecessary and avoidable.

45. Salmat notes that it will not always be practicable to include an opt out statement in each direct marketing communication. When adopting a multichannel communication strategy, organisations may choose to use a broad range of digital communication channels including twitter and/or mobile banner advertisements. The Bill needs to cater for all technologies/channels and be as technology neutral as possible.

RECOMMENDATION

46. Salmat submits that the language in APP7 revert to the language used in the Exposure Draft.

47. Salmat supports ADMA"s suggested amendments to APP 7.3 as outlined in their submission.

Outsourced service providers - APP 3-Collection of solicited personal information

48. APP 3 allows collection of personal information that is reasonably necessary for an entity"s activities. Clause 3.7 provides that APP3 specifically applies to "solicited" information, which is information an entity has requested an individual supply to it.

49. Salmat, is an outsourced service provider, covering many areas such as mailing services, bulk email communications and call centre operations. All of these activities are conducted on behalf of our clients, and as such, a large proportion of the personal information held by Salmat is collected by our clients, not by Salmat itself.

50. By way of specific examples - Salmat collects data from its clients for the generation of transactional mail items such as bank statements for the major banks, invoices for the major telecommunications companies, Medibank statements, Centrelink statements etc. All of this information is solicited - we ask for it from our customers in order to be able to perform the services we are contracted to perform.

51. Collection of this information from our customers is necessary for our activities. APP 3, via clause 3.6, also requires that personal information be collected **only from the individual.** For Salmat, this may not be the case - the information is passed onto us by our clients for processing. We assume that we could rely upon the exception that it is "unreasonable or impracticable" to do so (see clause 3.6(b)), but would appreciate clarification via an amendment to deal specifically with outsourced service providers.

52. In the case of sensitive information (ie: health information), the draft APP 3 requires that "the individual consents to the collection of the information". We expect that it is extremely unlikely that our clients, such as Medibank, Medicare and other health funds specifically seek the consent of the individual to the collection of the information by Salmat, as opposed to the initial collection by Medicare etc. In this respect, the legislation does not seem to cater at all for outsourced service providers like Salmat.

53. Conversely, when Salmat provides call centre services for a client, we may be required to collect personal information directly from an individual on behalf of that client. Salmat would then pass this personal information to the client (eg: Medicare or Centrelink). That client is potentially in breach of APP3 as it is not collecting the personal information directly from the individual.

54. Outsourced service providers are increasingly performing in house functions on behalf of their clients and acting as the client. Personal information will be passed from the outsourced service provider to the client and vice versa. It is essential that the Australian Privacy Principles explicitly recognise this business reality to put beyond doubt that outsourced service providers will not be contravening APP3 during normal operational activity.

Recommendation

55. Salmat submits that the APPs in some form should explicitly refer to outsourced service providers and the collection of personal information.

56. At a minimum, we propose that the word “and” be changed to “or” in clause 3.3 (a), or alternatively, that clause 3.3 (a) specifically apply only to “initial collection”.