Security concerns are top of mind for three in four Australians, who cite data breaches of their personal information at banks and credit card companies as a key concern. According to the Unisys Security Index, 74 percent of Australians said a data breach by accidental loss, theft or deliberate hacking at banks and credit companies was a cause for concern. Perhaps no surprise then that at the end of May, the Federal Attorney-General Mark Dreyfus QC, introduced new laws in Parliament which will require businesses and federal government agencies to notify people when a serious data breach affecting their privacy occurs. The new laws will also require notification of these data breaches to the Office of the Australian Information Commissioner. The Commissioner will be able to seek civil penalties if there is serious or repeated non-compliance with the notification requirements. iappANZ Board Director, Peter Leonard, writes on the objectives of the Bill and practicalities for organisations complying with the notification regime.

The introduction of the mandatory data breach notification Bill was then closely followed by Mr Dreyfus QC releasing the Terms of Reference requiring the Australian Law Reform Commission to conduct an inquiry into the prevention of, and remedies for, serious invasions of privacy in the digital age. For those of us who have questioned the pace of privacy law reform, evidence of how quickly...
things can get done when push comes to shove – or an election is on the horizon! iappANZ Director, Melanie Marks, provides an analysis on the proposed tort in this month’s bulletin and canvasses the uncertainties on its application.

Sally Stewart from National eHealth Transition Authority shares with us the use of drones or unmanned airborne vehicles by animal activists as a surveillance technique in the interests of animal welfare and how this fits within the right to privacy dialogue. A complex issue that revolves around how to strike a fair balance between the right to privacy and freedom of expression (in this case with the aid of some sophisticated technologies).

Moving on from protection of privacy by statutory tort, Annelies Moens, an iappANZ Director, provides her insights into the new EU Data Protection Regulation, proposed by the European Commission and currently being debated in the European Parliament. Just this week, media reports have surfaced from the European Court of Justice confirming that current EU laws do not mandate that internet search engines (i.e. Google) have to delete personal data from their search indexes. EU Advocate General Niilo Jääskinen has remarked that search engine service providers are not responsible, on the basis of the Data Protection Directive, for personal data appearing on web pages they process. Therefore under current laws, citizens do not have a right to be removed from search indexes within the framework of the Data Protection Directive. It will be interesting to see how this case impacts on the progress of the proposed regulation which mandates the ‘right to be forgotten’. A final judgment on the case is expected by the end of the year, although the ECJ is not bound by Mr Jääskinen’s decision.

We are fortunate to share a profile of Trevor Hughes, CIPP, President and CEO, IAPP on his role, privacy achievements and insights into the future. Finally, we also have our first book review this year from Andrew Calvin of Leif Gamertsfelder’s ‘Corporate Information and the Law’. We hope this inspires other members to share their thoughts on publications they may come across.

Kind regards
Anna Kuperman
Vice President, iappANZ

Footnotes:

1 ‘Data breaches top consumer concerns’ at www.australianbankingfinance.com on 27 May 2013.

2 Toby Sterling, ‘EU Court Rules That You Have No ‘Right To Be Forgotten’ By Google’ at http://www.huffingtonpost.com/2013/06/25/eu-court-google_n_3495450.html?utm_hp_ref=technology
In March 2013, the Government referred its proposed cause of action for privacy invasion back to the Australian Law Reform Commission (ALRC). The move was packaged up with a range of media reforms in response to the Convergence Review and the Finkelstein Inquiry.

The ALRC, which has already considered this question twice, has been asked to produce another report, due in June 2014. Terms of reference for the ALRC’s report were released in June by Attorney-General Mark Dreyfus QC, who has publicly expressed his concern about the adverse impact privacy litigation has had on freedom of speech in other countries. Given the arduous journey that the proposed tort has had since the ALRC first considered its introduction in 1979, privacy practitioners would be forgiven for wondering whether this move will be the speed hump which brings the proposed tort to a grinding halt.

The need for an enforceable common law right to privacy has been touted for several decades. Whilst some aspects of data protection are enshrined in the Privacy Act 1988, that statute is limited because it pertains to information privacy only (and not the protection of a person’s right of seclusion), offers a suite of exemptions and delivers complainants little in the way of compensation. The High Court in Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199; 185 ALR 1, famously stated that the ‘time was ripe’ for consideration of this issue. In 2008, the ALRC proposed the introduction of an action for serious privacy invasion as part of its review of privacy law in Australia. Finally, in the wake of the News of the World scandal, the Commonwealth Government in 2011 released for public comment an Issues Paper concerning the proposed tort, which it modeled on the ALRC’s work.

The cause of action was described in the Issues Paper in the following terms:

- To establish liability the claimant would need to show that in the circumstances there is a ‘reasonable expectation of privacy’ and the act or conduct complained of is ‘highly offensive to a reasonable person of ordinary sensibilities’;

- In making its determination, the court would need to consider whether the public interest in maintaining the claimant’s privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression);

- The action would only be available to natural persons;

- The action would be actionable without proof of damages;

- The action would be restricted to intentional or reckless acts by the respondent;

- Though no definition of ‘privacy’ or ‘privacy invasion’ was offered, a non-exhaustive list of the types of invasion that would fall within the cause of action was to be set out in legislation;

- Three defences would be available, being that the act or conduct was incidental to the exercise of a lawful right of defence of person or property, it was required or authorised by or under law or that under the law of defamation, publication was privileged; and
The court would be empowered to grant one or more of the following remedies: damages (including aggravated damages, but not exemplary damages); an account of profits; an injunction; an order requiring the respondent to apologise to the claimant; a correction order; an order for the delivery up and destruction of material; and a declaration.

Current views on the proposed tort

Legal Affairs Editor at The Australian, Chris Merritt has reported that media, business groups and state governments have responded to the framework outlined in the Issues Paper with concern that the initiative would expose them to a new wave of litigation. In his media release concerning the terms of reference for the current ALRC review of the proposed tort, Mr Dreyfus QC notes the risk of creating a more litigious culture amongst other possible issues raised by stakeholders during consultation. Given that the proposal is by nature the creation of a new right to sue (and noting current exemptions for journalism and state and territory authorities in the Privacy Act), this can hardly be surprising. What is surprising is that this point is being made now – after numerous rounds of input into the proposed cause of action.

The proposed tort has also been criticized for being so uncertain and subjective as to undermine the rule of law. Indeed, the proposal as described in the Issues Paper, leaves a large number of issues unanswered and some justifications for aspects of policy are not adequately substantiated. Three key areas of uncertainty include:

A) Definition of privacy/ invasion of privacy

Whilst there is a widespread understanding that the role of privacy in private law is to protect information privacy and seclusion, the boundaries of each and the precise situations in which an individual might have ‘reasonable expectations’ of privacy remain undefined. The difficulty of defining privacy has long plagued the judiciary, policy makers and commentators. In Giller v Procopets for example, it was stated that ‘the development of such a tort would require resolution of substantial definitional problems. This, of itself, might contraindicate such a development’.

The proposed cause of action does not address this uncertainty as its terms do not include a definition of what is ‘privacy’ or a ‘privacy invasion’. The action comprises a two part test, requiring the claimant to show that in the circumstances there was ‘a reasonable expectation of privacy’ and that the act or conduct complained of is ‘highly offensive to a reasonable person of ordinary sensibilities’. The Commonwealth also proposed that a list of types of invasion that fall within the cause of action be provided but that this list is non-exhaustive.

B) Freedom of expression versus privacy

That the proposed action might dampen free speech was one of the issues most commonly raised (particularly by media stakeholders) in response to various proposals for a privacy tort made by Commonwealth, NSW and Victorian Law Reform Commissions. It has similarly been flagged by Mr Dreyfus QC as an issue for consideration. The concern is that a statutory cause of action for breach of privacy would tip the balance too heavily in favour of privacy rights for individuals at the expense of the free flow of information on matters of public concern.
Under the terms of the proposed cause of action it is also unclear who bears the burden of demonstrating the public interest in being informed. In New Zealand, the defendant bears the onus of establishing there is a legitimate public concern in the publication of otherwise private facts. This is also the case under Canadian privacy law. However, in the USA, it is the plaintiff who must show that the matter is of legitimate concern to the public. Both the ALRC and NSWLRC proposals recommended that the plaintiff bears the burden, whilst the VLRC proposal preferred that the defendant carry it to prevent the plaintiff having to prove a negative. Although the Issues Paper canvassed these approaches, it was silent on a preferred position.

As noted above, our Attorney-General has signalled his personal view that while there are concerns about invasions of privacy, it is very difficult to legislate to enable privacy litigation without adversely affecting freedom of speech. In this interview, Mr Dreyfus QC said that countries that had created a statutory method of suing for privacy had failed to achieve the right balance with freedom of speech, noting that "Legislating in an effective way to protect privacy while at the same time not unduly affecting freedom of speech has proved to be a very difficult task.

C) The ‘highly offensive’ test

The second limb of the test proposed by the Commonwealth (that the act or conduct complained of is ‘highly offensive to a reasonable person of ordinary sensibilities’) has also brought debate given the perceived difficulty that a plaintiff would have in meeting this high bar. The ALRC itself shifted its position on this test, reflecting its uncertain suitability and indicating that this could be an area which causes confusion in practice. In its Review of Australian Privacy Law the ALRC expressed concern that the test might be too high a threshold and suggested that it be replaced with the question of whether the act in question was sufficiently serious to cause substantial offence to a person of ordinary sensibilities. However, following consultation, the ALRC accepted the higher bar, citing by way of explanation its concern in ensuring that freedom of expression is respected.

Terms of reference

This brings us to the current terms of reference for review of the proposed tort by the ALRC. Having considered the issue in its 2008 report, following the relevant New South Wales and Victorian Law Reform Commission privacy reports, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and in light of relevant Commonwealth, State, Territory legislation, international law and case law, the ALRC is charged with making recommendations regarding:

1. Innovative ways in which law may reduce serious invasions of privacy in the digital era.

2. The necessity of balancing the value of privacy with other fundamental values including freedom of expression and open justice.

3. The detailed legal design of a statutory cause of action for serious invasions of privacy, including not limited to:

   o legal thresholds;

   o the effect of the implied freedom of political communication;
o jurisdiction;
o fault elements;
o proof of damages;
o defences;
o exemptions;
o whether there should be a maximum award of damages;
o whether there should be a limitation period;
o whether the cause of action should be restricted to natural and living persons;
o whether any common law causes of action should be abolished;
o access to justice; and
o the availability of other court ordered remedies.

4. The nature and appropriateness of any other legal remedies for redress for serious invasions of privacy.

Conclusion
Has the proposed tort been brought to a grinding halt? Come June 2014, we may find that years of detailed consideration and consultation have led to its shelving or substantial reworking of its terms (again).

Melanie Marks is an iappANZ Director and privacy advisor to the National E-Health Transition Authority

Footnotes:

1 The second part of the test is drawn from American jurisprudence. Further, in Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199 (‘Lenah Game Meats’), Gleeson CJ at [42] referred to the second part of the test as ‘…in many circumstances a useful practical test of what is private’. Gleeson CJ’s adoption of this test was cited with approval by Lord Woolf in A v B Plc [2003] QB 195 and applied by the Court of Appeal in Campbell v MGN Ltd [2004] 2 AC 457 (‘Campbell’).

2 Examples given included an interference with an individual’s home or family life; an individual has been subjected to unauthorised surveillance; an individual’s correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or sensitive facts relating to an individual’s private life have been disclosed.
The latest David and Goliath story: Does the ‘right to be forgotten’ defy the tsunami of online information collection and distribution? By: Annelies Moens

The tsunami of personal information being collected, stored and processed online is growing and leaking in high volumes. Collecting and storing information used to be expensive, but not anymore.

Unstructured data sets, such as location information, clickstream data, sensors, server logs, social media, RFID and other meta data, fuel data mining activities. Public and private surveillance continues to rise with law enforcement entities sifting through information held by major online warehouses to which individuals contribute personal information.

It is in this environment that data protection laws are being enacted and amended. The Council of the European Union released on 31 May 2013 its proposed amendments to the European Commission’s draft regulation on data protection. The new ‘right to be forgotten’ proposed by the European Commission has been the subject of much debate and discussion. The Council of the European Union has not made significant changes to this proposed new right, but has made changes requiring the controller to act without undue delay when a data subject requests erasure. In relation to where the data is public and thus controlled by additional third parties, the controller can take into account available technology and cost of implementation in taking reasonable steps to inform third party controllers that a data subject requests erasure of their data:

Where the controller (...) has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take (...) reasonable steps, including technical measures, (...) to inform controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data.

In the Australian context, the concept of a ‘right to be forgotten’ is not entirely new and can be seen expressed in the Commonwealth spent convictions scheme under the Crimes Act 1914 (Cth) (and state and territory legislation) whereby after a period of years individuals do not need to disclose certain criminal convictions and unauthorised disclosure and use of this information is prohibited. Similarly, in credit reporting law contained within Part IIIA of the Privacy Act, there are requirements around erasure of defaults, bankruptcies, and new ‘positive’ information after a certain number of years. Australian businesses conducting business with European citizens will need to take heed of the ‘right to be forgotten’ as it moves closer towards implementation.

The concept of a ‘right to be forgotten’ on the Internet has significant social, legal and technical ramifications. There are many different perspectives that can be provided by archivists, technologists, data controllers and processors, media, lawyers and the individuals to whom the personal information relates.
The right to be forgotten may mean anything along a spectrum, including: a right to delete data held by sites and data brokers (arguably information created by the system, not the user), a right to delete information they themselves have authored and posted (possibly including the reposting of the information by another user), and/or the right to delete information drafted by another.\(^5\)

Complexities quickly arise from a technological point of view, as data is duplicated and hosted around the world and combined with other data. According to the European Network and Information Security Agency, the key technical challenges are:

(i) allowing a person to identify and locate personal data items stored about them;
(ii) tracking all copies of an item and all copies of information derived from the data item;
(iii) determining whether a person has the right to request removal of a data item; and
(iv) effecting the erasure or removal of all exact or derived copies of the item in the case where an authorised person exercises the right.\(^6\)

As always, the devil will be in the detail of the drafting of the ‘right to be forgotten’, which may be implemented in the European Union. The European Parliament’s Committee on Civil Liberties, Justice and Home Affairs is considering the amendments to the proposed Data Protection Regulation and preparing a compromise text for a European Parliament vote to be negotiated with the Council of the European Union.\(^7\)

It remains to be seen whether the ‘right to be forgotten’ is an effective and appropriate tool for individuals to control and manage the tsunami of online information collection and distribution of information about them.

**Annelies Moens** is Immediate Past President iappANZ and Head of Sales and Operations at Information Integrity Solutions, a global data protection and privacy consultancy. Annelies can be contacted at: annelies@iappanz.org

---

**Footnotes:**


2 Edward Snowden: the whistleblower behind the NSA surveillance revelations, (viewed 10 June 2013) [http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance](http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance)


4 Ibid p.61

Mandatory Data Breach Notification Scheme for Australia By: Peter Leonard

The Privacy Amendment (Privacy Alerts) Bill 2013 may be about to set a new privacy regulation record for speed from draft Bill to enactment\(^1\). This new haste remains unexplained by the Federal Government\(^2\). The Australian Law Reform Commission recommended introduction of a mandatory data breach notification scheme in its 2008 Report For Your Information: Australian Privacy Law and Practice. The Government never responded to that recommendation, but the Australian Attorney General released a discussion paper in October 2012 to canvas stakeholder views as to the introduction, and elements of, a mandatory data breach scheme\(^3\). Submissions were received and again not responded to by the Federal Government. Finally, after limited confidential consultations with a few stakeholders, the Bill was tabled in the Parliament without any prior Exposure Draft or other prior policy announcement. Following limited debate in the House of Representatives, the Bill went to the Senate and was referred to the Senate Standing Committee on Legal and Constitutional Affairs, which reported on 24 June 2013 recommending passage of the Bill\(^4\). Some 21 submissions were then made to the Senate Committee, many mixing complaints about the speed of the process and the underlying policy, with concerns as to uncertainties arising out of generalised drafting.

It is unfortunate that this important Bill continues the current Federal legislative practice of conflating discussion as to appropriate regulatory policy with legislative drafting to effect that policy. It is also unfortunate that the Federal Government did not announce its policy after acknowledging, or even take into account, the views of submitters expressed in response to the Governments’ invitation.

Important bills like this Bill should pass through an Exposure Draft phase, which enables potential issues to be identified and addressed before the Bill passes into political party partisan debates in the Parliament. Governments of both political parties at both State and Federal levels continue to make this error, with the result that legislation is enacted that is uncertain or difficult to apply and then regulators are left to try and fix the problems created by ill-considered legislative drafting through guidelines, regulations or codes.

That noted, the Bill on its face appears based on sound policy. According to the Explanatory Memorandum to the Bill, the policy rationale for the Bill is essentially two-fold: to ensure affected individuals can take action to mitigate any harm or loss they may suffer as a result of a data breach (the ‘mitigation’ objective); and to provide an incentive to entities holding personal information to adequately secure the information (the ‘deterrence’ objective)\(^5\).
It is difficult to quibble with either rationale. However, given that most OECD countries do not have mandatory data breach notification, the relevance of ‘deterrence’ as a policy objective of the new scheme deserves further scrutiny. The ‘deterrence’ objective assumes that the risk of reputational harm to an entity’s brand as a result of mandatory notification of data breaches incentivises the entity’s adoption of good privacy practices. Whether this is the case or not, the reality of online data storage practices is such that entities may suffer data breaches irrespective as to whether they have, or have not, complied at all times with the Privacy Act and taken all reasonable steps to protect personal information. As cyber-attacks become increasingly sophisticated, an entity that has deployed best practice information security may still suffer breaches as a result of malicious hacks. The Explanatory Memorandum to the Bill cites the well-known Sony PlayStation Network/Qriocity data breach and notes the Commissioner’s finding that Sony had in fact taken reasonable steps to secure the personal information concerned, but had nevertheless suffered a malicious cyber-attack.

Further, deterrence may be best effected through a coordinated response effected before notice is effectively given to the hacker that the cyber-attack has been detected. In other words, immediate notification to affected individuals may run counter to the consumer welfare objective of detection of the source of cyber-attacks and institution of effective counter-measures to ensure that they do not happen again.

Arguably, the ‘deterrence’ objective may be an appropriate policy objective for data notification schemes in jurisdictions in which entities are not subject to general privacy legal obligations to safeguard the personal information they hold – the States in the USA being a prime example. However, in jurisdictions such as Australia in which entities are already subject to strong legislative obligations relating to information security to protect of personal information – obligations which will be supplemented with enhanced OAIC enforcement powers from March 2014 – deterrence is of somewhat limited relevance as a policy objective of a mandatory notification scheme.

In any event, the Bill now builds on the OAIC’s scheme of voluntary notification of serious data breaches by entities, as set out in the OAIC’s Data Breach Notification: A guide to handling personal information security breaches. The Bill adopts a high threshold based on a reasonable belief by the entity concerned that the data breach is sufficiently serious to pose a real risk of serious harm to affected individuals. In the event of such a breach, the provisions of the Bill require the entity to notify affected individuals and the Information Commissioner as soon as practicable. The data breach notice must include:

the identity and contact details of the entity;
a description of the breach;
the kinds of personal information concerned;
recommendations about the steps that individuals should take in response to the breach; and
any other information specified in the yet-to-be made regulations.

The Bill expresses a preference for direct notification of affected individuals via the method/s of communication the entity normally uses to communicate with the relevant individuals. In the absence of such a method, the entity must take reasonable steps to notify the individual (e.g. by email, telephone or post). In circumstances, however, where it is impossible or impracticable to contact each affected individual, the Bill requires an entity to publish a copy of the statement on its website and in each State via publication in a
generally circulating newspaper in that State. The circumstances in which such indirect notification is to be undertaken is to be prescribed in the regulations.

Where it is in the public interest to do so, the Commissioner may exempt an entity by notice from its notification obligations. Such notices may be issued upon application by the entity or on the Commissioner’s own initiative.

The Bill also provides the Commissioner with the power to direct an entity to notify affected individuals if it has not done so. A failure to comply with the notification requirements of the Bill, as well as a direction by the Commissioner to notify, amounts to an interference with the privacy of an individual, which triggers all the Commissioner’s enforcement powers, including the investigative powers, the power to make determinations, award compensation, seek enforceable undertakings and civil penalties for serious or repeated interferences with privacy.

Submissions to the Senate Committee highlighted three key areas:

uncertainty as to the meaning of the phrase ‘real risk of serious harm’ within the definition of ‘serious data breach’;

the order of the steps to be taken in mandatory notification; and inclusion of exceptions to the mandatory notification provisions and their alleged breadth.

Regulated entities (which do not include SMEs) are likely to face a number of challenging practical issues in their efforts to comply with the new scheme, not least of which will be determining whether there are reasonable grounds to believe that there has been a serious data breach in respect of personal information it holds. The Bill is not helpful as to the meaning of the term ‘serious harm’, noting that it includes reputational, economic, financial, physical and psychological harm, but excludes minor harm. The ALRC Report also provides little assistance on this issue, noting that, in another context, the term ‘real risk of serious harm’ has been defined to mean a reasonable degree of likelihood, real and substantial danger, and a real and substantial risk. Consistent with the approach taken in relation to other nebulous concepts in the Privacy Act, the Explanatory Memorandum contemplates that the Commissioner will provide further guidance on the meaning of this standard. The Attorney-General’s Department submitted to the Senate Committee that the standard is “a commonly understood concept amongst agencies and organisations that have sought to comply with the OAIC guide and emphasised the flexibility of the OAIC guide to adapt to specific contexts and to evolve over time. The OAIC advised the Senate Committee that if the Bill proceeds, ‘the OAIC will prioritise the amendment of the [OAIC guide] to address and provide clarity on the operation of the new mandatory notification requirements’. However, while accepting that OAIC guidance does have the benefit of potential flexibility, the absence of legal standing for that guidance potentially creates exposure to privacy class actions against regulated entities for breach of statutory duty even in circumstances where they followed OAIC guidelines. And of course there is still no Government commitment as to adequate resourcing of the OAIC, with the result that these and many other guidelines will need to be produced by relatively few staff members.

Another aspect of the Bill requiring OAIC guidance (still noting its legal limitations) is the application of the notification obligations for a data breach that occurs in the context of outsourcing arrangements: for example, where a storage service provider located in Australia holds personal information on behalf of the original collecting entity. Once a data breach occurs, which of the entities is responsible
under the scheme to notify the affected individuals: the outsourcing entity or the service provider, or both? The OAIC Guide helpfully suggests that, in such circumstances, the entity with the direct relationship with the affected individuals should notify. The situation, however, is less clear under the Bill. The provisions of the Bill are drafted on the basis that a serious data breach will occur in relation to an APP entity (for example) that holds personal information. Under the Amended Act, an entity holds personal information if the entity has possession or control of a record that contains personal information. If a serious data breach occurs in respect of the information held by the entity, then the Bill deems that breach to be ‘a serious data breach of the APP entity in relation to the personal information’. It is unclear how this then applies in an outsourcing context, in which the service provider suffers a serious data breach. In these circumstances, is the breach a serious data breach of the service provider only, or is it a breach by both the service provider and the outsourcing entity on the basis that both entities may possess or control the personal information concerned to varying degrees?

Arguably the notification obligations would then apply to both entities in respect of the same data breach. Perhaps the reasonable steps qualification to notification would provide grounds for only one of the entities undertaking notification of the affected individuals. Specifically, an entity might argue that it is not reasonable in the circumstances to notify the affected individuals as the entity with the direct customer relationship has assumed responsibility for such notification. Alternatively, an entity might apply to the Commissioner for a notification exemption on the basis that it is not in the public interest for both entities to notify affected individuals about the same data breach.

Under the proposed new mandatory data notification scheme, entities holding personal information that is the subject of a data breach are responsible for determining whether the circumstances of the breach are such that affected individuals, and the Information Commissioner, must be notified under the scheme. There is some merit to this approach as the entity is itself best placed to assess the nature of the breach, the risks that might arise for affected individuals, appropriate mitigating action affected individuals should take, and the most appropriate method of communicating the notification. However, in fulfilling their statutory duty, entities will face a number of difficult practical questions around the severity of the harm that affected individuals may face as a result of the breach. This will probably lead to over-notification, at least to counter concerns as to possible media criticism, or exposure to class actions, for failure to notify.

Perhaps the most important privacy regulatory initiative of the last few years has passed through the Federal Parliament in about three weeks, and will doubtless lead to a substantial increase in the volume of the OAIC’s inbox. Privacy regulation now moves in mysterious ways.

Peter Leonard is an iappANZ Director and partner of Gilbert + Tobin Lawyers

Footnotes:
The Bill was introduced by the Federal Attorney-General, the Hon Mark Dreyfus QC MP, in the House of Representatives on Wednesday 29 May 2013. The Bill, and its Explanatory Memorandum, are available here: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5059


Explanatory Memorandum to the Privacy Amendment (Privacy Alerts) Bill 2013 (Cth) page 5.

EM, 5.

ALRC Report, [51.10].

Privacy Alerts Bill, s 26ZB(1).

Ibid.

Ibid, s 26ZB(3).

Ibid, s 26ZB(h).

Ibid, ss 26ZB(5)-(7).

Ibid, s 26ZC.

Ibid, item 3.

Explanatory Memorandum, 2.

R v Secretary of State for the Home Department; Ex Parte Sivakumaran [1998] AC 958.

Explanatory Memorandum, 57.


Amended Act, s 6 (definition of holds).
In the Public Interest of Animal Welfare. By Sally Stewart

More than a decade since the High Court handed down its judgment in *ABC v Lenah Game Meats Pty Limited* animal rights activists are continuing to employ questionable surveillance methods in the interests of animal welfare.

In April this year, Animal Liberation announced the purchase of an airborne surveillance drone equipped with a powerful camera that it proposed would be flown over Australian farming areas in an attempt to monitor farmers’ treatment of livestock.

Understandably, many farmers were outraged at the suggested intrusion, with NSW Farmers and other industry bodies seeking legal advice on whether or not the practice would be an invasion of privacy or otherwise considered a trespass.

Commenting on the question of privacy, Executive Director of Animal Liberation Mark Pearson stated “If there is public interest, then that is not an invasion; it is a service to the community. The High Court has already dealt with the issue of privacy. We’re not interested in people’s personal lives and what’s happening in their homes, but if you have a business which uses animals then that is of public interest, and that’s been dealt with by the High Court.”

Although the line between public interest and any potential invasion of privacy may not be as clear as Mr Pearson suggests, the proposed practice of using a privately operated commercial drone for the purpose of monitoring the treatment of animals on farming properties is not illegal.

Current Australian law does not provide corporations (including farmers) with a right to privacy and for a farmer to prove trespass they would need to show that the drones interfered with their use and enjoyment of the land. Drones or unmanned airborne vehicles (UAVs) are currently treated as aircrafts by the Civil Aviation Safety Authority. For this reason, as long as the UAV operates more than 10m from the ground and does not film in any private homes, no laws are being broken.

Commercial use of UAVs can be beneficial for farming and agriculture. They can be used for aerial photography, fire control, crop and livestock monitoring and search and rescue. But with the increasing availability and relative affordability of UAVs, the question of their...
regulation must be addressed as existing surveillance laws do not apply. Academics and various law reform commissions, including the Australian Law Reform Commission, have highlighted the inadequacies of the common law in providing individuals with sufficient legal protections from these newly developing technologies. Their recommendation has uniformly been a statutory right of privacy, however developments in this area are a long way off with the Commonwealth Government referring the question back to the ALRC for further consideration.

Some of the questions that need to be addressed in relation to the operation of UAVs are: What data are they collecting? How is it being stored? What is it being used for? Who will have access to the data? How can operators be held accountable for unreasonable, unlawful or excessive uses? And what remedies should be available to aggrieved consumers?

In September 2012, Australian Privacy Commissioner Timothy Pilgrim said that "the potentially intrusive nature of the technology" meant that there should be a public debate about regulating the use of UAVs. Mr Pilgrim wrote to the then Australian Attorney General urging her to review the current regulatory framework to ensure that individuals who may be subject to any misuse of this technology have access to appropriate redress under the law.

UAVs are not the only form of surveillance adopted by animal rights campaigners. In June this year, claims have been made that activists trespassed on private property and illegally filmed at two piggeries near Young in NSW. Mr Pearson says Animal Liberation obtained the footage taken from the two farms and that they support activists breaking the law to get evidence of what he calls animal cruelty. Whilst the farming methods adopted by both these NSW piggeries are legal and comply with all relevant industry standards, there are some cases where these surveillance methods have exposed illegal practices and this year at least one NSW abattoir has been shut down as a result.

The type of footage obtained in these circumstances certainly generates significant public interest. It is a normal human response to become distressed when seeing animals dying, even when it is done so lawfully. As Sir Paul McCartney once said "If slaughterhouses had glass walls, everyone would be vegetarian". But the public’s right to be exposed to these practices must be balanced with a farmer’s right to privacy and their ability to conduct their business in a lawful manner.

Whether or not Animal Liberation is justified in using lawful surveillance technology to expose particular farming practices is a matter for debate. What is clear is that current Australian laws governing the unlawful surveillance or misuse of UAVs must be updated in order to address the new technologies that are emerging all the time. For Australians to realise the potential benefits of these technologies, the associated risks need to be identified and managed within a robust legal framework.

**Sally Stewart** is a Senior Privacy Advisor with the National eHealth Transition Authority

1. *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63; 208 CLR 199; 185 ALR 1; 76 ALJR 1 (15 November 2001)

2. Farms generally operate as a Company, Partnership or Trust rather than as an individual.
A lawyer's work revolves around information - obtaining instructions from clients, storing that information, and ultimately using and re-using it. That information will be affected by some or all of the laws of copyright, consumer protection, insider trading, misuse of information and privacy, as well as obligations imposed by equitable confidentiality, stock market rules, EU directives, litigation, contracts, financial disclosure rules, data retention requirements and finally, the need to destroy it when it is no longer required.

In *Corporate Information and the Law*, Gamertsfelder notes that “information has value.” There are many many organisations today whose only market value is in the quality and quantity of the information they own. We want our banks to have correct information that is closely guarded, but we want our government to have information freely available. Each organisation needs an information governance framework that suits the needs of it and all its stakeholders. Designing and implementing that framework is now a key obligation of business managers, and the design needs to be based on an understanding of the information, relevant laws and best practices.

Gamertsfelder has addressed the key topics within a discussion of risk in the modern enterprise - an entirely appropriate approach given the financial and criminal penalties that can apply to infringers. This is a practical book for lawyers and information owners and managers, citing cases and legislation extensively, with a large bibliography. It is not a technical book in the computer sense - the technical issues can be addressed once the governance matters are agreed.

Privacy is addressed bearing in mind the amendments to the *Privacy Act 1988* that will take effect in March 2014, ensuring that the book remains relevant on this topic for some years. It is a good primer on privacy obligations in Australia, but it goes deeper into topics that are just starting to emerge. Does your laptop have a fingerprint reader? Many do, and if your organisation implements it, how is this biometric information dealt with by the Act? I suspect it won’t be long before phones and tablets use biometric data to unlock them (Android can use facial recognition today) and implementing these features is no longer just an IT challenge.

While there is detailed examination of the *Corporations Act* and the ASX Listing Rules, the discussion is sufficiently broad that it will take some time to date. The chapter “Disclosure and Investor Protection” is a useful introduction for a lawyer becoming involved in a public company for the first time, or issuing a prospectus or drafting a bidder’s or target’s statement. A lawyer involved in financial services might be well-advised read this to understand the wide range of matters affecting a client’s conduct and disclosure.

The book also deals with the withholding of information - when can you refuse to disclose, and when does an organisation lose privilege?

Cybersecurity has been in the news of late, and it really is an umbrella term for being a good shepherd of all the obligations discussed in the book, such as privacy, contractual, fiduciary, and legislative and what to do when it all goes wrong. A data breach requires expert assistance in several areas, and it must be provided quickly and accurately - you only get one chance to get it right.

A common question from clients is whether they need to produce paper records, as well as keep them, or can they scan and discard them? The chapter explains retention obligations, evidentiary issues, production and inspection for regulators, and some of the
penalties. This again is a good starting point for an internal discussion about information management in the enterprise. Too often it is seen as just a technical challenge, when actually the technology is finally the easy part. The hard part is getting the policies, processes and people all working together. *Corporate Information and the Law* is a contemporary and very useful review of Australian law for any lawyer or information owner.

**Andrew Calvin** is Senior Legal Counsel, Sydney Water Corporation

---

**iappANZ Profile Trevor Hughes, CIPP, President and CEO, IAPP**

**What kinds of issues keep you awake at night as IAPP President and CEO?**

For the IAPP, the explosive growth of the field of privacy is the most compelling challenge we face. The organization has been growing by approximately 30% per year for a number of years. With 10,000 members in 2012, we now have 13,500 in 2013 – with more growth happening daily! Responding to our members’ needs, developing programs for an international audience, building bigger and bigger events – all of these challenges keep us very busy at the IAPP.

**How do you think Australia and New Zealand are faring in their data protection laws?**

Australia and New Zealand clearly have a mature and robust public policy and enforcement structure for data protection. But like all jurisdictions around the world, data protections laws struggle to respond to the ferocious speed of technological innovation. The burgeoning privacy profession is one of the most important mechanisms to manage this “gap” between existing law and marketplace practice. And in that regard, I think IAPP ANZ is doing a great job promoting and building the profession.

**Favourite app and why?**

I travel a lot, so I use FlightTrack and Google’s Map app all the time

**Your biggest achievement in privacy?**

Without question, leading the IAPP from a very small professional association of 300 members to a global organization. I am tremendously proud of the work we have done to support the growth of this field. And we are not done! I look forward to the years ahead with even more energy and enthusiasm.

In a prior role, I also led an industry group working on standards for email marketing and another working on behavioural advertising in the United States. The email group ensured that the CAN SPAM Act in the US provided important privacy protections, while allowing legitimate marketing to continue. We also introduced and championed the idea of authenticated email. It was challenging work, but I think we created a workable environment where privacy and data flows were protected.
What was the highlight for you at IAPP’s conference this year?

The IAPP’s Global Privacy Summit can be an overwhelming event. We have 2500 attendees, almost 100 sessions, a huge exhibit floor, and thousands of details to address. In the middle of that whirlwind, I find the greatest satisfaction in the personal connections that I create and re-invigorate. The global privacy profession, despite our incredible growth, is still a relatively nascent field. So we find great value and satisfaction in the friendships we create with each other. Those connections provide the glue that keeps our profession together. I could spend the entire conference standing next to the coffee pot and still go home feeling like I received phenomenal value from the event.

Favourite global city and why?

Unfair question! There are too many favourite cities. I can walk around Paris, Rome or London for days happily. Toronto is the city that I grew up close to, and I always love returning there. San Francisco, Boston, Hong Kong, Singapore, Amsterdam, Madrid – they all have special appeal for different reasons. And, in my mind, Sydney might be tied with Vancouver for most beautiful city in the world. Basically, I like finding local coffee shops and art galleries when I travel for business and have a few hours to myself. That combination – coffee and art – adds up to a “good” city in my mind!

What are you reading at the moment?

A few histories of the industrial revolution in the UK and US. I am trying to see if there are lessons for the information economy from the upheaval created by the introduction of the industrial economy. The industrial economy led to many societal reforms – standardized working conditions, women’s rights, urbanization, and environmental concerns. I think there are some lessons for the privacy community in that history.

The next big thing in privacy is .....?

Complexity. We continue to see efforts for legislative frameworks and policy solutions to the concerns created by data in society. But what we see within the IAPP is an ever-increasing complexity in the management of data-related risks for organizations. I do believe that we will have new laws in the years ahead, but I think that they will be one vector in a very complex matrix of privacy risks that professionals need to manage.

What are you tweeting about?

I generally tweet from conferences I attend. I like the “meta” conversation that gets created at an event.

What advice do you have for privacy professionals today?

Embrace the role and the profession! We are in the beginning years of what will become of a critical profession in the information economy. We need leaders to bring ferocious curiosity, clear thinking and innovation to the field. That will require us to band together as a profession and learn from each other. Joining, participating, and volunteering in IAPP ANZ; getting certified; and continuing to
devour privacy knowledge – all are critical to professional development and to our ability to effectively manage privacy in the years ahead.

**Win a cash prize: iappANZ’s writing prize 2013**

iappANZ is very excited to announce the launch of a new [$250 cash] writing prize for an article that is published in our monthly Bulletin between February and October 2013. Anyone can enter (you don't have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy. Opinions are most welcome but nothing too extreme.

All articles must be submitted by email, preferably in Word, to kate.johnstone@suncorp.com.au or an admin@iappanz.org by 20 October 2013. We will need the author’s email address and contact number. You can submit as many articles as you like. Email Kate Johnstone if you have any questions.

The winner will be announced at our Privacy Summit on 25 November 2013 and their name and details will be published on our website. [We also hope to publish profile of the winner in our Bulletin].

So alert your network and get writing!

More details about the writing prize if you are interested:

- Our Editorial team, Kate Johnstone, Veronica Scott plus President Emma Hossack and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.
- Articles submitted and published in the February, March and April Bulletins will also be eligible for the prize – we don't want anyone who has already made a valuable contribution to miss out.
- Some people won't be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.
- After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky not to be at our Summit.
- There will (sadly) be one prize only. Its value is AUS$250, so that’s pretty good really.
- We may need to verify the winner's identity so we don't give the prize to the wrong person.
- If the prize is not claimed for any reason (and we hope this won't happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

To make sure things go smoothly and fairly (and we are sure they will) we just have to say that our decision in relation to any aspect of the award of the prize, including the content and publication of submitted articles, is final and binding and not up for discussion.
Upcoming Privacy Events

**Australian Cyber Security Forum, Melbourne 26 and 27 August 2013**
The Australian Cyber Security Forum is the only dedicated independent cyber security conference in Melbourne, targeting senior IT and security managers with the latest tools, strategies and best practices needed to stay ahead of the rising cyber threat landscape.
As a member of iappANZ you will receive 10% discount on verification of your membership. For more details see: http://www.aventedge.com/event-details/?eid=164

**Health Informatics Conference 15-18 July, 2013**
Book in to hear privacy presentations from Dr Trish Williams and iappANZ President Emma Hossack
Go HIC’s website for more details of the conference which will take place in Adelaide this year.

**The University of Auckland Business School, proudly supported by iappANZ and KPMG, invites you to a presentation by Malcolm Crompton on The cloud, big data, analytics and data losses**

*Date:* Friday 19 July 2013  
*Time:* 6pm  
*Venue:* The University of Auckland Business School, Decima Glenn Room, Level 3, Owen G Glenn Building, 12 Grafton Road, Auckland

Big data analytics promise huge, unexpected benefits, from curing cancer to new business models and intimate service. The revolution has only just begun and there will be some scary pitfalls along the way. Join us to hear privacy expert Malcolm Crompton, Managing Director of Information Integrity Solutions (IIS), founding President of iappANZ and former Privacy Commissioner of Australia, discuss how big data analytics might be used to change our lives safely and what to do when the cloud, big data, analytics and data losses surround us all.

Big data depends on vast amounts of personal information being collected, shared and analysed by organisations that are not necessarily familiar. And it's not just our names, birthdates and addresses – it's our moment-by-moment location, who is nearby, who we are talking to, what we are buying, when we turned on the shower and lots more. The only way this revolution can be delivered efficiently is through cloud computing platforms, with their own pitfalls and challenges. The change will be incredibly disruptive, but will we let this happen? The answer lies in trust.

We must trust that the information will not be lost or stolen, that it will not be used to harm us or discriminate against us or manipulate us. We need to trust that when the inevitable happens and things go wrong or mistakes are made, there is justice and somebody to
make things right. Malcolm will take us on a whirlwind tour of the issues and suggest that we can have our cake and eat it too.

Since he established IIS in 2004, it has advised Government agencies, global ICT companies and many others on data protection and privacy strategies to increase business value and customer trust through the way they handle personal information. Malcolm has advised APEC on its privacy framework since 2003 and as Australia’s Privacy Commissioner from 1999 to 2004, he led the implementation of Australia’s private sector privacy law. Malcolm was the Foundation President of the International Association of Privacy Professionals Australia New Zealand in 2008 and a Director of the IAPP for five years until 2011.

Malcolm is a member of the Microsoft Trustworthy Computing Academic Advisory Board and has been a member of external reference groups for large research projects funded by the European Union. Malcolm’s global reputation and expertise in privacy was recognised when IAPP honoured Malcolm with the 2012 Privacy Leadership Award.

Proudly supported by iappANZ and KPMG

Please register by clicking on this link: https://secure.business.auckland.ac.nz/MalcolmCromptonPresentation

Recruitment

Standard Chartered Bank is hiring 2 Global Privacy Analysts in Singapore

Working in the Bank’s Data, Technology & Operations Group L&C (DTO L&C) team based in Singapore and London, the role holder will, as a member of a bigger team of lawyers and privacy professionals of varying seniority, be responsible for corporate oversight of privacy policies, practices and procedures across global operations.

This role will be a key resource in the Global Privacy Programme and serve as a data privacy consultant to in-country and global business lines, and support functions (e.g., information technology and human resources) by providing expert advice and guidance across the Bank on all strategic privacy projects and on BAU projects and requirements.

Please click here for a detailed description.

IAPP Certification

Privacy is a growing concern across organisations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, privacy certification provides you with internationally recognised evidence of your knowledge, and it may be the edge you need to secure meaningful work
in your field.

The International Association of Privacy Professionals (IAPP) says:

“In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.”

What certifications are available? Are they relevant to my work here?

The IAPP offers four credentials, one of which is particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT).

To achieve this credential, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for distinct IAPP privacy certifications – in our case, CIPP/IT.

CIPP/IT assesses understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.

What about testing?

Although the IAPP website refers to US-based certification testing only, testing is available to iappANZ members locally.

The IAPP will continue to manage certification registrations and materials, but you will now be able to set an appointment to sit your exam online at a testing centre in Australia or New Zealand.

FIND OUT MORE HERE

Back to Top