Data Sovereignty

Patrick Sefton[*]

Legalwise In-House Counsel Conference, 22 March 2013

Introduction

Data is a high-value organisational asset. Data generated and stored by organisations is also increasingly exposed to misuse. This paper examines the law surrounding the control and protection of data as an organisational asset.

Background

There is a lot of data.

Google Inc's executive chair Eric Schmidt famously commented that "every two days, we create as much data as we did from the dawn of civilization up until 2003."[1] Although much of the growth in bare volumes of data is driven by individuals, particularly in relation to video content, there is also substantial growth in the volume of data generated, stored and used by organisations.

Data is a high-value asset. An organisation's overall data store typically contains confidential information and trade secrets which would be of value to competitors. Data represents fruits to the organisation of expensive effort (for example, customer lists and intelligence). Data will likely also contain essential, irrecoverable records of the organisation (in particular, financial records). Data may represent and evidence regulatory compliance (for example, in the form of tax records). Data stores may evidence contractual relationships and performance (for example, transactional records and records of correspondence including email). Finally, organisational data may include overall organisational history, including correspondence, which will comprise evidence in the case of later legal dispute: as litigators like to say, "the record is reality," so in the case of litigation, the strength of an organisation's position may depend on the quality of its data store.

Organisational data can itself generate further value to an organisation through analysis. The concept of "big data" has become clichéd in the technology sector and with venture capitalists. Nevertheless, data analysis and consulting services are being started and funded to take advantage of growing quantities of corporate data and the challenges of its analysis.

Changing technology landscape

As a result of growth in data, and its treatment within organisations, organisational data is also exposed to misuse. A number of changes and developments have contributed to that exposure.

In particular, the broad connectivity brought by the internet allows data to be easily moved between sites, organisations and recipients quickly and easily: most desktops and laptops are internet-connected and need to be in order to facilitate productive work. High capacity, portable storage media such as USB memory sticks have become ubiquitous.

---

[*] Principal, Brightline Lawyers.

[1] Comments at the *Techonomy* conference in Lake Tahoe, CA, United States, 4 August 2010.

In addition, the internet era has seen a move to electronically exposing an organisation's internal data – previously only available to more carefully managed access from within the organisation. It is no-doubt highly convenient for consumers to be able to, for example, check bank balances, track delivery of packages and manage airline bookings online. However, in the process, data can become incorrectly exposed. Many information privacy breaches are the result of careless over-openness, rather than deliberate malicious hacking.

Further, data networking is increasingly built-in to all kinds of equipment which was not previously connected. Printers and scanners typically have network, wireless, and often remote access facilities for maintenance, built-in to their basic operation. Networking equipment is also becoming more sophisticated, and simple devices are increasingly being supplied with their own web-site maintenance pages, and login and password functions, which are open to abuse if not properly managed.

In research published this month, anonymous[2] researchers were able to connect to and take control over more than 400,000 internet-connected devices such as laser printers, as well as network infrastructure such as routers, by the simple expedient of using unchanged default logins and passwords such as "admin."[3]

Portable and personal devices

There are a huge variety of portable devices: principally mobile phones and tablets. From 2012 the volume of phones and tablets manufactured annually has exceeded the corresponding volume of PCs and notebooks.

Portable devices are also usually internet connected and with high-capacity storage. More importantly, mobile devices can frequently connect to data networks through the mobile phone system, circumventing organisational border protections such as firewalls, anti-virus and intrusion detection systems.

Portable devices such as tablets and phones are also more personal devices than notebooks. They are correspondingly less likely to belong to the organisation itself, and more likely to belong to individual employees who wish to use their own device, rather than being issued a similar but generic device by their employer. Bring-your-own-device ("BYOD") policies are becoming common in the workplace.

By way of example, listed banking and insurance group Suncorp is an industry-leader in the BYOD and desktop virtualisation area through its "smart environments" initiative.[4,5] The initiative arose out of the 2010 Queensland floods, when Suncorp needed to send a large number of employees home for an extended period, and subsequently to remote locations to service claims. Suncorp invested heavily in developing a virtual desktop usable on a number of different devices, as well as access to Suncorp network features from employees' own portable devices. In mid-2012, Suncorp announced that it had over 1,000 users on a BYOD and virtual desktop pilot, with a target of 100% of its relevant workforce within 18 months. Suncorp reported a direct translation of these policies into fewer individual PCs and workspaces (at a saving of

---

[2] Anonymous because in most jurisdictions, particularly the US, the researchers have engaged in serious criminality by accessing devices which are protected by passwords.

[3] *Internet Census 2012 – port scanning /0 using insecure embedded devices*, <*http://census2012.sourceforge.net/paper.html*>.

[4] Computerworld, "Suncorp Banks on desktop virtualisation," 6 March 2012 <*http://www.computerworld.com.au/article/417556/suncorp_banks_desktop_virtualization/*>.

[5] IT Wire, "BYOD and virtualisation saves Suncorp dosh, " 18 July 2012 <*http://www.itwire.com/business-it-news/networking/55764-byod-and-virtualisation-saves-suncorp-dosh*>.

$15,000 per workspace, and 50% less in ongoing costs) and flow-on real-estate savings from reduced floor space requirements.

Data misuse and "cybercrime"

With these increases in portable storage and connectivity comes increasing exposure to organisational data to negligence and malice.

In one recent Australian survey of large organisations,[6] it was reported that 22% of organisations know they experienced a "cyber incident" (defined as an electronic attack that caused actual harm) in the 12 months preceding the survey. The reported consequences of such attacks were: 17% of organisations lost information or had confidential information compromised (including on lost or stolen devices or media), 16% encountered a denial of service, and 10% were subject to financial fraud.

In relation to the sources of such malicious action, from another survey[7] only approximately 11% of data loss attacks are deliberate attacks from insiders within an organisation, though other exposures may be caused by insider carelessness.

Although certainly widely reported and certainly a significant issue for organisations to address, it is unclear whether "cybercrime" overall is increasing over time, because it is difficult to locate reliable independent information. Many published reports originate from security software vendors, who have an obvious commercial interest in ensuring the threat is well-understood, and can tend to sensationalise.

"Ownership" of data

Although organisational data is a valuable business asset, strictly data is not property. An organisation's rights arise from the intellectual property in its data, principally copyright and rights in confidential information. However, data sometimes does not sit comfortably in either of these areas, and organisations must be careful not to assume that data is automatically protected by either regime.

Copyright

Copyright was originally intended to protect individual creative work, not data, no matter how valuable. Uncertainty has resulted from attempts to apply copyright to protect investments in organisational data, simply because the circumstances in which such data is created are not the circumstances in which copyright traditionally arises, that is, in relation to literary, artistic or musical work.

---

[6] *2012 Cyber Crime and Security Survey: Systems of National Interest*, CERT Australia and the Centre for Internet Security, 2012.

[7] InfoSec Island, "Hackers Overtake Insiders as Leading Cause of Data Loss," 22 April 2011, <*http://www.infosecisland.com/blogview/13282-Hackers-Overtake-Insiders-as-Leading-Cause-of-Data-Loss.html*> reporting survey by Identity Theft Resource Centre.

Desktop Marketing,[8] **IceTV,**[9] **Phone Directories Company**[10]

The line of telephone book cases (and the Ice TV program guide case) well illustrates the risk of assuming that merely because data has taken cost and effort to compile, it will be protected from copying by a competitor.

Legally, these are copyright disputes, but substantively they are disputes about the right to control and exploit organisational data, in this case very large and valuable compilations of phone directory data. Copyright is the blunt (or at least, antiquated) instrument by which data owners must take action to protect their data and their investment in compiling it.

Before about 2009, Australia did have a "sweat-of-the-brow" theory of copyright in application to collections of data. Provided a collection had taken time and effort to create or compile, it did not matter that it was not "original" or "creative" in a literary sense. (The opposite result applied in the US, again in phone directory cases such as *Feist*[11], where some degree of creativity or originality was required for protection).

The *IceTV*[12] case was a dispute about the content of on-line TV guides. TV scheduling data was assembled by Channel Nine, which data Nine considered to be its own property by virtue of "the sweat of its brow," ie, that it had expended time and effort in creating the schedule. The schedules included program title, broadcast time, format, classification and brief synopsis. Nine communicated the schedules to "aggregators" such as TV Week magazine. Aggregators would publish weekly aggregated guides for all channels.

IceTV maintained its own scheduling database, initially populated from actual broadcast details (that is, IceTV paid people to watch TV and take notes about what was on), and then undertook a process called "check & change" from Nine's published schedule – updating its own database from that information.

Nine sued for infringement of copyright in its schedules.

IceTV ultimately won in the High Court, essentially on the basis that copyright in Australia offers very little protection for collections of facts: the more limited the creativity and originality in the work, the more limited the protection would be against copying (and IceTV had copied only "slivers" of not-very-original information).

The *Phone Directories Company* case[13] followed IceTV to find that there was no copyright in Telstra white and yellow pages directories. Authors must direct "independent intellectual effort" or a "sufficient effort of a literary nature." Where there is no "authorship" or "originality," copyright does not subsist, no matter how much effort has gone in to creating the data, or how valuable it is.

Keane CJ explained very directly, "the focus of attention … is *not upon a general concern to prevent misappropriation of skill and labour* but upon the protection of copyright in literary works which originate from individuals" (emphasis added).

---

[8] *Desktop Marketing Systems Pty Ltd v Telstra Corporation Ltd* [2002] FCAFC 112 (15 May 2002) (special leave refused 20 June 2003).

[9] *IceTV Pty Ltd v Nine Network Australia Pty Ltd* [2009] HCA 14 (22 April 2009).

[10] *Telstra Corporation Ltd v Phone Directories Company Pty Ltd* [2010] FCA 44; *Telstra Corporation Limited v Phone Directories Company Pty Ltd* [2010] FCAFC 149.

[11] *Feist Publications, Inc v Rural Telephone Service Co* 499 U.S. 340 (1991).

[12] Above, note 9.

[13] Above, note 10.

Practical consequences for organisations

Organisations should not assume that a database or data collection is protected by copyright, just because it is valuable or because it has taken time and effort to compile.

Copyright protection is difficult to apply to organisational data stores, particularly stores of facts such as customer contact information. A database owner needs to show that there was some degree of independent creative effort in creating the content of a database, including identifying individual authors, in order to qualify for copyright protection. Simply showing the database is valuable, or cost money to create, is not enough.

Confidential information

The law of confidential information and trade secrets can be applied by an organisation to protect its data from misuse by others. Three elements must be established[14,15] in a claim for breach of confidential information (assuming there is no additional contractual obligation of confidence). The information concerned must:

- be identified with specificity, and not merely in global terms;
- have the necessary quality of confidence (ie, it must be genuinely confidential);
- have been imparted in circumstances identifying an obligation of confidence;

There must also be an unauthorised use (or threat of such use) of that information to the detriment of the person who claims the confidence.

All of the elements can be contentious.

For example, although specific identification of the relevant information may seem straightforward enough, in *Manderson*[16] a business data confidentiality claim was lost because the information concerned was not (after multiple attempts by the plaintiff) sufficiently identified. In that case, the information to be protected was a leasing-related business and financial model, which was alleged to have been misappropriated by the Incitec Pivot Ltd, following a powerpoint presentation given to it by Manderson.

Manderson had four attempts at pleading the claim, each of which was struck out for the above reason, and ultimately summary judgment was awarded to IPL. The problem was that the business model in question was only illustrated and shown in operational examples in the claim, rather than being "identified with specificity." The claim never actually stated what the data (ie, the model) *was*, only what it achieved.

Practical consequences for organisations

The second and third elements, those of information being genuinely confidential and imparted in circumstances of confidence, raise some important practical issues for organisations.

---

[14] *Coco v AN Clark (Engineers) Ltd* (1968) 1A IPR 587; *Commonwealth v John Fairfax & Sons Ltd* [1980] HCA 44.

[15] *Corrs Pavey Whiting & Byrne v Collector of Customs* [1987] FCA 266.

[16] *Manderson M & F Consulting (a firm) v Incitec Pivot Limited* [2010] VSC 63 (9 March 2010).

To show information is genuinely confidential, an organisation may need to show what real, practical steps it takes to maintain the confidential nature of its information. So, for example, an organisation may need to show that copies of its information are closely controlled and not distributed to others (at least, without an appropriately serious warning or agreement as to their confidential nature).

To show information was imparted in circumstances of confidence, again practical steps should be taken to notify recipients that information is confidential and proprietary. For example, written warnings and confidentiality notices on the front cover of materials and presentations, appropriate contract terms regarding confidentiality, sensible and practical security procedures to control and audit the distribution of information, should all be considered by an organisation in respect of its confidential data. As well as having a practical deterrent effect, taking such steps improves the prospects of successful enforcement action should it be required.

Lawful access to data

In addition to malicious access and IP rights infringement, organisations will also be concerned about managing the scope of lawful access by others to their data. There are a number of ways in which lawful access can occur: the following is intended to be a brief reminder rather than an in-depth analysis of each process.

- **Disclosure** in litigation. A party to proceedings will need to comply with disclosure obligations. Clearly a challenge for large organisations is to manage the process and comply with obligations across possibly many kinds of data including correspondence and electronic files. Sophisticated e-disclosure tools are available. Obviously issues of relevance and privilege must be managed.

- **Non-party / preliminary discovery**. The Federal Court Rules and some States' (but not Queensland's) UCPR enactments allow for preliminary discovery

  In *Sony v University of Tasmania*,[17] the applicant music companies obtained identity discovery orders against several universities in order to identify individuals who were using university facilities to distribute infringing music files. The main issue in this case was that the orders sought by the rights owners – to obtain forensic copies of relevant systems – would go far beyond records relevant to the infringement (ie, they would be access records of everyone who used the relevant systems). In the universities' view it was effectively a fishing expedition. It was held that there was also an interest in full and proper preliminary discovery in order to ensure that an informed decision can be made as to whether to commence proceedings and against whom they should be brought. On this basis, and on the basis that there would be strong confidentiality undertakings protecting the data provided and analysed, the broader discovery was ordered.

- **Subpoenas**. These must be specific, they cannot be oppressive or a fishing expedition. Organisations which regularly receive subpoenas should have a system in place for assessing, tracking and responding to them (as well as costing compliance), and including applications to set-aside where necessary.

  Note that the Queensland UCPR does not contain preliminary discovery / identity discovery rules. A subpoena is required (eg, for identifying the proper defendant). However subpoenas will not be issued by a Queensland court unless there are already proceedings on foot: the registry will not issue "bare"

[17] *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 532 (30 May 2003)

subpoena to obtain identity discovery. The correct process is to make an originating application for the subpoena to be issued, naming the relevant record holders as respondents.

- **FOI** (for relevant organisations). Again, relevant organisations should have a responsible officer and system for tracking and responding to requests.

- **Individuals' personal information** under NPP6, IPP6, APP12. Individuals' right to access their own personal information under privacy law is continued in the recently passed reform package. Again, organisations which frequently receive such requests should have an officer to track and deal with such requests.

- **Civil search orders** (what used to be called Anton Piller orders) under Chapter 8, Division 3 of the UCPR. The first an organisation will know of this kind of order is a heavy knock at the door. There is usually little option but to comply with the order. Organisations are entitled to hold the search while they seek legal advice, assert privilege, and can make an urgent application for the order to be set aside if it is an abuse or was otherwise not properly made in the ex parte application.

Law enforcement access to data

Law enforcement access to data is less common, but should still be a consideration for large organisations, particularly telecommunications carriers and ISPs. Carriers and ISPs typically have an agency liaison function, by which they manage official requests for access to data in the course of investigations. The author has recently had cause to deal with agency liaison in several carriers, and they have been extremely helpful.

The following is a survey of law enforcement and security services channels to access organisational data in the course of investigations:

- **Queensland Police**, s153 *Police Powers and Responsibilities Act 2000* (Qld) provides that a warrant may order production of documents, or (s154) order a person to give access to a storage device and the access information necessary for the police to use the device to gain access to information. This is directed towards having an appropriate person provide logins and passwords to allow the police to access it.

  The AFP has similar powers.

- **Other enforcement agencies**, for example the ACCC has civil search powers under Part XI D of the *Competition and Consumer Act* (Cth). The ACCC can access electronic equipment at the searched premises, require assistance from persons, print documents, take a forensic copy of data, or seize equipment if cannot print or copy data (s154H). The ACCC's powers have been used very sparingly. For example, in their first 5 years of operation, it executed 10 warrants.

  An organisation which has is the subject of an ACCC search should: check the warrant (the subject is entitled to a copy), ask the ACCC to wait for legal advice to be sought (they don't have to wait, but there is no harm in asking), observe the search (the subject is entitled to observe, so long as they don't interfere), assert privilege (privileged documents should be kept from investigators until the privilege claim is resolved).

Overseas law enforcement agencies access to data

There was some contentious debate in 2011 when Microsoft launched its Office 365 cloud product and was asked whether, because they were a US company, international customers' data would be subject to US government agency access under the USA PATRIOT Act.[18] Microsoft confirmed that it would.

The "library records" provision of the Patriot Act allows access to records of entities located in the US, or which are US-based, including access to non-content data (so-called meta-data) about communications by means of "National Security Letters" and without warrant or judicial oversight. Further, the Foreign Intelligence Amendments Act grants the US government powers to collect foreign intelligence information stored in the US or by US entities, including providers of public cloud computing services.

Although there was some surprise at the outcome, it is likely that even in the absence of the Patriot Act US agencies would still be entitled to access US-based cloud provider data. Other countries including Australia have those rights in respect of Australian entities, including to seek data from overseas locations stored by entities within the jurisdiction. In *Bank of Valletta v NCA* [1999] the Federal Court required an Australian branch of a foreign bank to produce overseas documents in Australian criminal proceedings.

Australia is party to a number of mutual legal assistance treaties allowing access to data for the purpose of criminal investigations. In particular, Australia recently ratified the *Council of Europe Convention on Cybercrime* through the *Cybercrime Legislation Amendment Act 2012* (Cth). The Act amended certain Commonwealth cybercrime offences and enabled domestic agencies to access and share information relating to international investigations. The Act also provides for carriers and ISPs to preserve data where requested by domestic authorities, or by nominated foreign countries, and to seek access to that data under warrant.

In December 2012, the US Ambassador to Australia, Jeffrey Bleich, wrote an opinion piece in the Sydney morning Herald calling for an end to "cloud protectionism," – the apparent desire for data to be stored in local data centres rather than offshore-based centres. He strongly suggested that free trade agreements should require no barriers for data between domestic and offshore data centres and cloud providers, and that Australian customers should be comfortable with US cloud providers storing data in the US.

Google now publishes the number of data requests it receives from law-enforcement, worldwide, in its bi-annual Transparency Report. Google receives around 40,000 requests per year, from all agencies in all countries, of which 1,100 per year are from Australian agencies. Approximately 65% of requests result in some data being provided.[19]

Practical steps in response to law enforcement requests

Organisations should review requests to ensure the request complies with legal requirements. It should at a minimum be made in writing, signed by an authorised official of the requesting agency, and issued under an appropriate law. Where requests are overly broad, an organisation should seek to narrow them by discussion with agency concerned. Although there is no legal obligation to do so, it is likely appropriate (unless prohibited by the request or order) to notify affected individuals where possible.

---

[18] Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001 (United States of America).

[19] Google Inc Transparency Report at *http://www.google.com/transparencyreport/userdatarequests/*

Agreements with others

In addition to exposure from malicious attackers and insiders, lawful access, and domestic and international law enforcement, there is also a commercial risk to data arising from transactions and services arrangements with other organisations.

The following could be used as a checklist to ensure that data sovereignty is preserved through dealings with another organisation which may involve the provision or exchange of data.

- Confidentiality (specifically identify the confidential material and assert confidentiality both in the agreement and on the face of each confidential document, or where data or reports are accessed);
- IP Rights including in improvements during the course of the arrangement;
- Return of data on demand or on expiry or termination of the agreement. It is often practically useful to have the completeness of the return (ie that the other party has not retained any documents) certified by a senior officer of the other organisation;
- Deal with how an orderly transition will occur to a new/replacement partner;
- Deal with what will happen on insolvency of the other party, ie, that the data is proprietary and will be returned;
- Assurance of regulatory compliance, notification and reporting of data incidents such as breaches, access requests or subpoenas.

Outsourcing / cloud arrangements

In outsourcing or cloud arrangements, an organisation's data may be placed wholly under the responsibility of an external provider. The hope is that the external provider will have greater expertise in the area of data security, so reducing the risk. However, additional risks are introduced: in particular the reduction in control and the risk of dispute with the external provider itself.

Question is: is the additional skill and expertise of the cloud provider worth the additional risks of trusting the data to an external party? Follow-up question: what objective certification / due diligence can be obtained to be sure the provider is reliable? (eg, PCI)

If an organisation does propose to outsource data functions to a service provider, the governing contract is a crucial component of preserving the organisation's sovereignty over its data.

Important aspects of the contract, so far as data is concerned, are the following:

- Pre-contract due diligence, certifications, standards compliance (PCI-DSS, Uptime Institute Tier);
- Standards and security – warranties against certification;
- For commodity / consumer oriented services (Google Drive, Dropbox, iCloud) check to determine whether the "take it or leave it" click-wrap standard terms contain unacceptable ownership or licence provisions. Google was criticised when it initially launched its Drive product, on the basis that the terms allowed a Google a broad licence to communicate, publish and display all data stored.

However, the licence is limited to operating, promoting and improving the service. Nevertheless, it may still be inappropriate for even mildly sensitive information;

- Availability metrics, service levels or KPIs, and associated remedies;
- Details of physical location, assurance that data will be kept in-country (or in any particular country);
- Confidentiality: as discussed above, it is important to state the nature of confidential information clearly to preserve the capacity to enforce confidentiality rights;
- Privacy Act compliance if data includes personal information (in specific terms, that is, the provider will take at least reasonable steps to protect security of information, there will be no trans-border data flows, the provider will not provide the data to any other person).
- Backup/DR – who is responsible, are any additional facilities required (depending on value of data). Obtain a copy of the provider's DR plan, and consider how it applies to your organisation's data. What is your organisation's DR plan if the provider suddenly disappears?
- Reporting, for example, data breaches, subpoenas, law enforcement access requests;
- Periodic copy of the data should be provided (either a full copy or an incremental backup). Alternatively, access to the system should be allowed to take a copy. The copy should be in a readable public format (not the provider's proprietary format);
- Appropriate notice periods, for example, to terminate or renew;
- Delivery-up of data on expiry / termination (in a public format, on standard media);
- Transition out assistance (though it can be difficult to contract for genuine assistance – there is also a need to mitigate the risk by maintaining an external copy of the data);
- The provider should have no lien and no destruction rights (or circumstances where lien, destruction will occur)
- What happens on change of control or insolvency?

When planning to change providers, organisations should ensure they have a copy of their data in-hand before advising of the proposed change and requesting transition-out assistance, as risk mitigation. There are some providers which will treat data as a bargaining piece in negotiating renewals or transition costs.

Data Liens

A cloud or data centre provider may be able to place pressure on or extract commercial concessions from an organisation merely by virtue of holding the organisation's data. Some outsourcing or cloud providers seek to enforce contractual liens on data to secure payment of fees. This will be of particular concern where it is proposed to change provider, or where there is a dispute.

Clearly a proposed contractual lien should be considered carefully, taking into account that the value of an organisation's data (and therefore the value of the security) will normally far exceed the costs secured by it.

In the absence of a contractual lien, it would be extremely difficult for a provider to prove a lien at common law: *Majeau v Coastal Rutile*[20] traverses the numerous authorities in detail. An implied possessory lien requires satisfactory proof of some actual custom of trade, and must be certain, lack ambiguity, be reasonable, and be "so notorious that everybody in the trade enters into a contract with that usage as an implied term." In the case of cloud and outsourcing service providers, the industry is relatively new, and there is unlikely to be sufficient standard approaches to support an implied lien. A provider which asserted such a lien would do so at considerable risk (for example, of mandatory injunction proceedings to deliver the data).

It *might* be possible for a provider to claim a statutory lien under *Storage Liens Act*,[21] given the broad definitions of "goods" and "storer" in that legislation. Ideally, an organisation should exclude any lien in their agreement with the provider.

Conclusion

Increasing data volumes and technological changes have resulted in risks to a key and highly valuable organisational asset – the organisation's data. This paper has surveyed a large number of risks and access pathways which may imperil an organisation's sovereignty over its data. However, there are also outlined a number of practical steps which an organisation can take to mitigate those risks.

[20] *Majeau Carrying Co Pty Ltd v Coastal Rutile Ltd* [1973] HCA 22 (7 August 1973).

[21] *Storage Liens Act 1973* (Qld)