office of the privacy commissioner
new south wales

Own motion inquiry / investigation

Rail Corporation of New South Wales (RailCorp)

Privacy and Personal Information Protection Act 1998 **June 2012**

This report is made pursuant to section 36(2)(l) of the NSW *Privacy and Personal Information Protection Act 1998* (PPIP Act) and placed in the public domain as the NSW Privacy Commissioner's[1] public statement pursuant to section 36(2)(h) of the PPIP Act.

Part 1: Introduction – The scheme of general functions of the Privacy Commissioner

Sections 36 and 37 of the PPIP Act confer on the Privacy Commissioner various functions regarding privacy issues and principles. These functions include making inquiries and investigations into privacy related matters as the Privacy Commissioner thinks appropriate,[2] requiring public sector agencies to provide information and documents in connection with the Privacy Commissioner's functions[3] and the making of public statements about any matter relating to the privacy of individuals generally.[4] The Privacy Commissioner does not have determinative powers and can only express opinions and make recommendations.

Part 2: The privacy obligations of RailCorp

On 1 January 2009 RailCorp was reconstituted as a statutory authority (it was previously a State owned Corporation), and as a result became subject to the Information Protection Principles (IPP's) under the PPIP Act.

IPP 5 is contained in section 12 of the PPIP Act. Relevantly it provides that when dealing with personal information,

> **12 Retention and security of personal information**
>
> A public sector agency that holds personal information must ensure:
>
> (a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
>
> (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and
>
> (c) **that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse**, and
>
> (d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.
>
> *(emphasis added)*

[1] The words Privacy Commissioner appear, they are intended to encompass the exercise of functions as Deputy Privacy Commissioner, exercising functions under delegation from the Privacy Commissioner.
[2] PPIP Act section 36(l).
[3] PPIP Act section 37(1).
[4] PPIP Act section 36(h).

Part 3: The process of the inquiry

Members of the public may occasionally lose items of property while using the public transport system. RailCorp operates public trains and has a process whereby it sells various goods found on train carriages and other areas of its facilities by way of public auction.

One such type of lost and unclaimed property is USB memory devices (USBs).

A **USB flash drive** is a data storage device that includes flash memory with an integrated Universal Serial Bus (USB) interface.

In early December 2011 a website operated by a staff member of an internet security company reported along the lines that company staff had purchased a number of USBs at one of RailCorp's auctions for purposes of research. The website also reported along the lines that, after examination by data recovery software used at the company, a significant volume of information was recovered and this included files containing personal information.

The issue was also reported in the mainstream print and digital media.

On 7 December 2011 the Privacy Commissioner responded publicly to the reported issues in broad terms.

On 9 December 2011 the Privacy Commissioner notified RailCorp of the commencement of inquiries under the PPIP Act. The Privacy Commissioner requested RailCorp to provide responses to various questions. The central issue of concern was to evaluate RailCorp's processes for cleansing data from any USBs sold at auction.

On 20 December 2011 RailCorp provided responses to the Privacy Commissioner's questions.

After making arrangements with RailCorp, in February 2012 the Privacy Commissioner observed the USB cleansing process at one of RailCorp's facilities.

During an attendance at the internet security company's offices in March 2012 as part of the investigation and information gathering process the Privacy Commissioner provided to the company sample USBs for the purpose of demonstrating the recovery process. Senior staff of the company provided an oral presentation about the potential risk of data recovery on memory devices considered cleansed. The company also provided a demonstration of the data recovery process they used and provided electronic copies of data recovered from sample USBs.

In early April 2012 the Privacy Commissioner issued to RailCorp a copy of a draft report for comment.

RailCorp responded on 18 April 2012 indicating that having reviewed the draft report, they had no comment to make as to its content.

Over the intervening period the Privacy Commissioner and RailCorp discussed the public release of the draft report as a final report and placed in the public domain as the Commissioner's public statement pursuant to section 36 (2) (h) of the PPIP Act. The draft report is now published as the final report dated June 2012.

Part 4: Evaluation of RailCorp's cleansing process

RailCorp submitted that:

Lost property is kept at the RailCorp location where it is found for a period of time and, if unclaimed, it is transferred to RailCorp's lost property office where it is kept for a further period of time.

If still unclaimed, it is transferred RailCorp's auction room.

Each lost USB is screened for information that may assist RailCorp return it to its owner. If an owner is identified, RailCorp attempt to contact that owner for the return of the USB.

If the owner cannot be identified, RailCorp delete the data on the USB and check to ascertain whether the data was erased before offering the USB at auction.

In recent times RailCorp offered USBs at auctions in July 2009, September 2010 and September 2011.

The Privacy Commissioner's observations during the demonstration at RailCorp's office were that RailCorp staff insert the USBs to be cleansed in a standard desktop computer with the WINDOWS operating system and follow a data deletion process commonly known as "long format." The Privacy Commissioner understands that this process is available on any WINDOWS based computer, whether at a work or home environment, and that it is designed to

write indecipherable data over the files that existed on the USB. The Privacy Commissioner observed, and RailCorp staff confirmed, that RailCorp did not utilise specialised data deletion software.

The Privacy Commissioner's observations during the data recovery demonstration at the internet security company's office was that the company used data recovery software, which was said to be inexpensive and commonly available.

The inquiry process leads the Privacy Commissioner to understand that:

RailCorp's USB cleansing process is unlikely to enable data to be recovered by re-inserting a USB into a standard computer with WINDOWS or MacIntosh operating systems and trying to open files.

Specialised data recovery software have the capacity to extract data from USBs that have undergone the data deletion process, which was used by RailCorp and which is commonly available on WINDOWS based computers.

Such specialised data recovery software is readily available and is relatively inexpensive.

The data recovery process that the Privacy Commissioner's inquiry process observed at the company's premises appears somewhat time consuming, but not cumbersome to a degree that might discourage a person intent on data recovery.

During the Privacy Commissioner's attendance at RailCorp premises as part of the investigation process, RailCorp staff advised that RailCorp had reviewed the risk that its deletion process presents to the personal information on the USBs and had concluded that the additional cost and labour time required to eliminate it would render auctioning the USBs economically unviable. For this reason RailCorp advised that it had decided to cease the practice of auctioning unclaimed USBs and adopt a practice of safe disposal by way of secure destruction of the USBs.

Part 5: Conclusion

During the process of the Privacy Commissioner's inquiries, no evidence was uncovered which established the actual disclosure of personal information, tied with a complaint by an individual who had standing to assert that their privacy rights under the PPIP Act had been breached.

In this regard the Privacy Commissioner makes no findings in respect of a breach of section 12 of the PPIP Act.

It seems clear from the matters raised in the public domain by purchasers of USB keys at 2011 RailCorp public auctions, that 3rd party personal information was allegedly accessible to the purchasers.

It seems clear also that had the original data on the USB keys contained personal information, then the processes in place to cleanse the data and meet RailCorp's obligations under section 12 (c) of the PPIP Act were insufficient for that purpose.

Taking into account the limitations of the existing 'cleansing' process, the potential risks to the Agency in this aspect of their operations when managing their privacy obligations under the PPIP Act, coupled with the economic necessity for RailCorp to run its lost property operation on a cost recovery basis, it seems prohibitive to the Privacy Commissioner for RailCorp to continue to offer such portable date storage devices (USB keys) for sale.

The Privacy Commissioner considers that RailCorp's assessment of the risk to the privacy of individuals is correct and that the decision to cease auctioning USBs is the most reasonable outcome.

The Privacy Commissioner commends RailCorp's decision, made without waiting for the completion of this inquiry.

John McAteer
Deputy Privacy Commissioner
Information and Privacy Commission

13 June 2012