Privacy of Personal Information – An audit perspective.

Wendi Watkins – November 2013
Independent Audit and Risk Services Limited

It’s happening everywhere

EQC admits another privacy breach

By Rebecca Quilliam

7:42 PM Tuesday Sep 17, 2013

Save

The Earthquake Commission has admitted to another breach of privacy after information on up to 260 claimants was sent to the wrong customers.

Kiwibank apologises after privacy breach

By Nicholas McBride of the Greymouth Star -

3:27 PM Friday Oct 11, 2013

Save

Kiwibank has apologised to all customers affected by a privacy breach at the Greymouth branch.

An envelope full of confidential documents was handed to a member of the public when they went into the Post Shop office last month.

The individual took it home and opened it, unaware of what was inside, before nents to a

ACC admits another privacy breach

Updated at 9:24 pm on 14 August 2013

ACC has defended the time it took to inform clients their personal information wa home in the fourth major privacy breach involving the corporation in just under tw

Nurse suspended for privacy breach

WILMA MCCORKINDALE

Last updated 19:12 17/09/20

Motorists' privacy breached

RICHARD MEADOWS

Last updated 05:00 22/09/2013

14 Share

Thousands of motorists have had personal details sold to third parties, despite explicitly asking for privacy, more than two years after the law was changed to protect their information.

The New Zealand Transport Agency operates the Motor Vehicle Register, which records information about vehicles and their owners, including names, addresses and dates of birth. In May 2011, drivers were given the choice to "opt out" from having their details publicly available.

Assistant Privacy Commissioner Katrine Evans said one of the main catalysts was companies using addresses for direct marketing, but there were also real risks for individuals.

Google fined for data privacy breaches

Monday 30 Sep 2013 1:24p.m. Join the discussion

EMAIL

WINZ: privacy breach 'major stuff up'

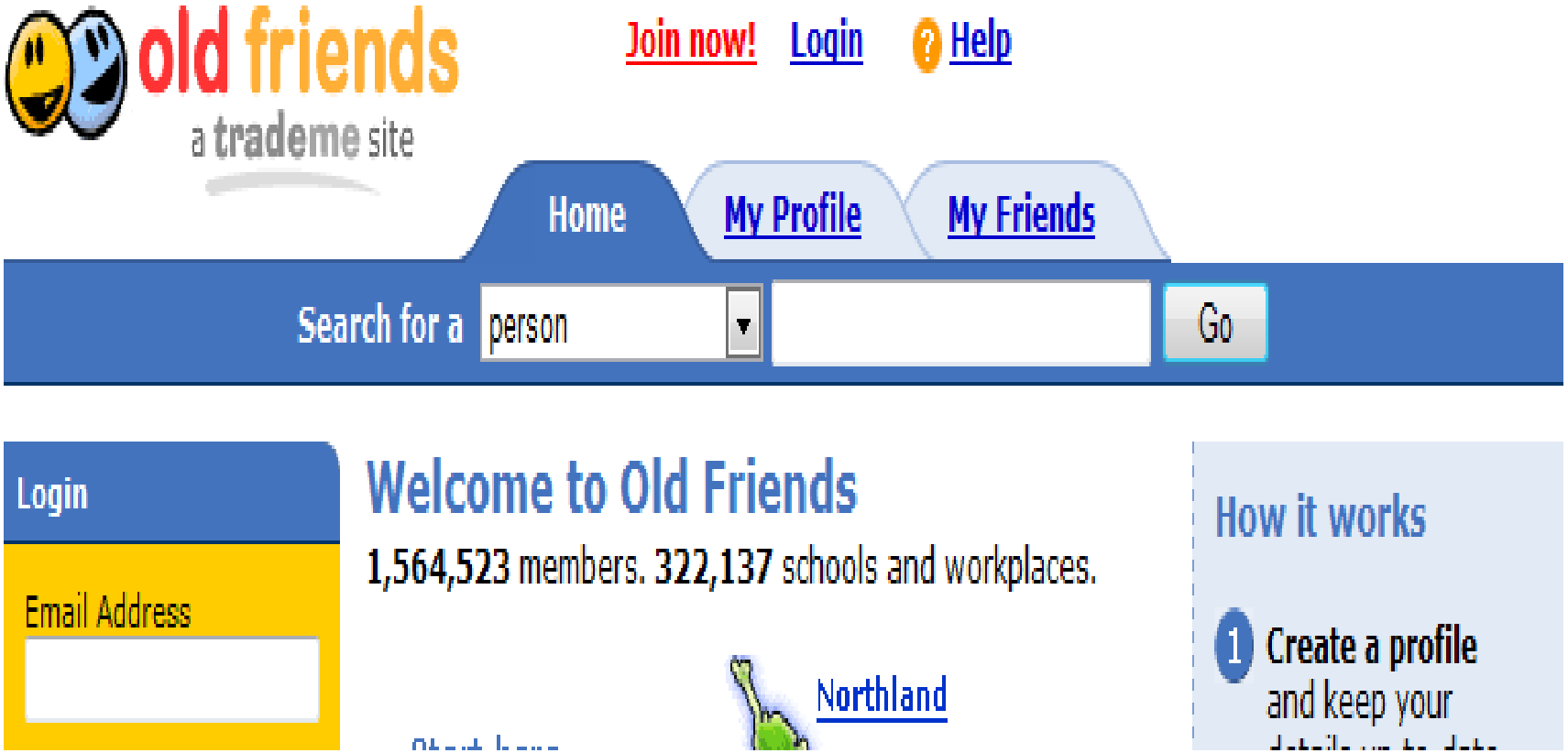
By Michael Morrah Reporter

Saturday 18 May 2013 6:00p.m.

000 for breaking r

Join

Ever seen this site?



How private is your information?

[redacted] attended from 1983 to 1985

1. hi my name is [redacted] i loking for [redacted] not sure if he did go to this school

   Posted by [redacted] Sun, 14 Sep 2008

2. He was at Mana College when I was there. He was definately there in 1984 and possibly 1985 as well. Though I haven't met him in over 20 years I did have dealings with his family and they tell me he is still in Porirua.

   Last saw campbell in 1985

   Posted by [redacted] Tue, 16 Sep 2008

3. would u no how 2 get hold of him a

   Posted by [redacted] Thu, 18 Sep 2008

4. By law I cannot give the information about how to contact him as the information was obtained when I worked for WINZ. But he is in Porirua still. Try the electoral roll for MANA. It'll have the details.

   Posted by [redacted] Sat, 11 Oct 2008

5. If its [redacted] who folks lived at Hukatai St Elsdon...then yep I know where he is ..[redacted]

   Last saw [redacted] in 2009

   Posted by [redacted] Wed, 11 Mar 2009

6. Yes it is that one if your [redacted] the last time i saw him was in about 1986-87 when he give me a ride home. [redacted] thank you

   Posted by [redacted] Wed, 03 Jun 2009

7. Is'nt he in jail?

   Posted by [redacted] Sun, 26 Sep 2010

It can happen to you!

- Accidentally violated others' privacy?
- Ever forwarded a sensitive email to the wrong person, or sent an incorrect attachment?
- It can happen to anyone.

Why things seem to be worse?

What's contributing to this

- Society demands that the public sector offers a one-stop, joined-up, value for money service and at the same time, keep all information concerning individuals secure.

- It's important to recognise that protecting personal information comes at a cost.

Assessing your organisation

- Objective of audit:
  - Assess the adequacy and effectiveness of the management of personal information by company xyz.
- Criteria:
  - NZ Privacy Act 1993

Governance

- Ownership and leadership at the top of the organisation.
- Direction provided around standards and values expected.
- Reporting to those standards.

Leadership

- The CEO and Senior Leadership team are actively involved in ensuring the development, implementation and promotion of privacy measures throughout the organisation.

Privacy Programme

- There is an enterprise wide programme in place, including plans, annual risk assessments, procedures, guidelines, training, checklists, quality reviews and reporting.

Accountability

- Key roles are in place for leading the work required.
- Accountability is also assigned throughout the organisation to staff and management.
- Responsibilities are understood and monitored against requirements.

Culture

- Culture is one where people value and respect personal information.
- The behaviours and beliefs of the organisation and those within it.
- Systems are in place to report concerns, learn from issues and these are fed back into improvements in the business.

People, Processes and Systems

- Organisational Policies have privacy embedded.
- They are accessible.
- There is a programme of review including sign off at appropriate levels.
- Issues are fed back into policies.

Communication

- Communication channels are secure and minimise inadvertent communication of personal information.
- Communication to customers is in place so that they know their rights and how the organisation will care for their information.
- Consequences for mishandling are well communicated.

Rating scale used

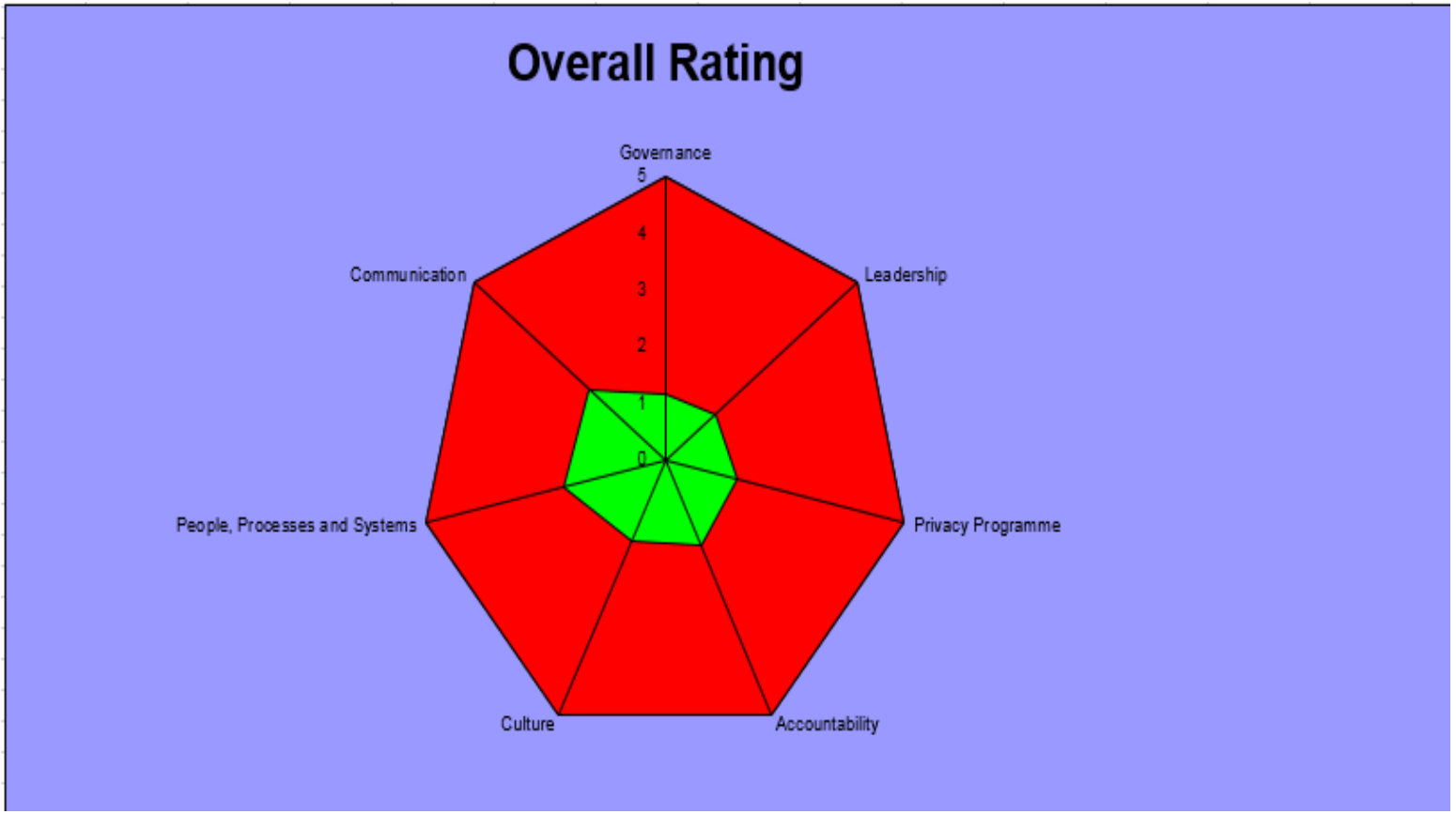
Privacy Maturity Model		
1	Ad Hoc	Procedure or processes are generally informal, incomplete, and inconsistently applied.
2	Repeatable	Procedures or processes exist; however, they are not fully documented, do not cover all relevant aspects and are not fully understood by staff.
3	Defined	Procedures and processes are fully documented, implemented, cover all relevant aspects and are understood by staff.
4	Managed	Reviews are conducted to assess the effectiveness of the controls in place.
5	Optimised	Regular review and feedback are used to ensure continuous improvement towards optimisations of the given process.
		Taken from AICPA Privacy Maturity Model

Charting the results

Chart Legend

Colour	Interpretation
Green area	Current performance against better practice
Amber area	Difference between current performance and expected future performance against "better practice" (assuming that current initiatives are fully implemented in the short-term)
Red area	Difference between current or anticipated future performance against "better practice"

Overall rating on core areas



12 Privacy Principles:

- Principle 1 – Purpose of collection of personal information.

- Principle 2 – Source of personal information.

12 Privacy Principles:

- Principle 3 – Collection of information from subject

- Principle 4 – Manner of collection of personal information

12 Privacy Principles:

- Principle 5 – Storage and security of personal information.

- Principle 6 – Access to personal information

12 Privacy Principles

- Principle 7 – Correction of personal information.

- Principle 8 – Accuracy of personal information to be checked before use.

12 Privacy Principles

- Principle 9 – Retention - Agency not to keep personal information for longer than necessary.

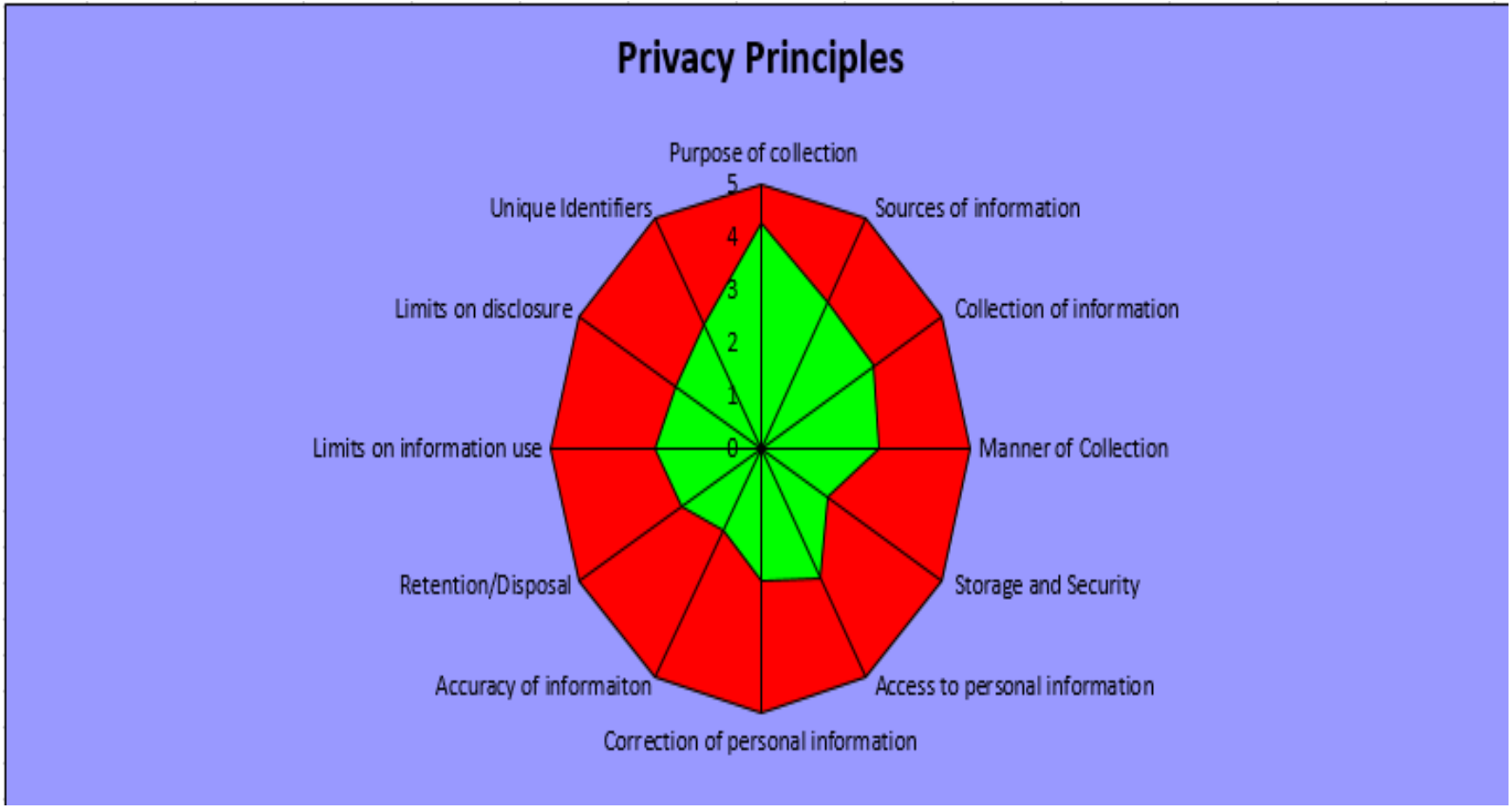
- Principle 10 – Limits on use of personal information.

12 Privacy Principles

- Principle 11 – Limits on disclosure of personal information.

- Principle 12 – Unique identifiers.

Overall rating on Privacy Principles



How they scored

Attributes	Better Practice	Now
Governance	5	1
Leadership	5	1
Privacy Programme	5	2
Accountability	5	2
Culture	5	2
People, Processes and Systems	5	2
Communication	5	2
Purpose of collection	5	4
Sources of information	5	3
Collection of information	5	3
Manner of Collection	5	3
Storage and Security	5	2
Access to personal information	5	3
Correction of personal information	5	3
Accuracy of information	5	2
Retention/Disposal	5	2
Limits on information use	5	3
Limits on disclosure	5	2
Unique Identifiers	5	3
	5	
	Average	2.90

Overall results

- Foundations of a privacy programme with a Privacy Officer who manages complaints received from the Office of the Privacy Commissioner, supports the business when requested.

- Pockets of expertise mainly at the Customer Service Centre.

Overall results

- Privacy of personal information has not had a coordinated focus.
- There is no governance processes including at a Board level.
- There is limited accountability and responsibility.

Overall results

- No culture of “privacy by design” and “privacy by redesign”.
- No clear understanding of risks to organisation.
- No clear business rules and guidelines on how to manage.

Things aren’t standing still

- Panel of security service providers to help government agencies manage privacy and security issues effectively.

- Panel to provide external expertise and advice on the strength and suitability of their ICT security processes, or to test the security of their ICT systems.

Things aren’t standing still

- Bill to give more powers to the Privacy Commissioner

- Bill not passed

Value for our organisations

- Privacy Act provides a roadmap
- We can measure our organisations
- Baseline for measurement in future periods

Questions