CLENDONS
BARRISTERS & SOLICITORS

Data Matching and Privacy Laws in New Zealand

An introduction to the laws surrounding the collection and use of personal information for data matching.

Contents

For more information on matters covered
in this paper, please contact:

James Carnie
Principal
DDI: +64 9 306 8002
Email: james.carnie@clendons.co.nz

Jasmine Smart
Solicitor
DDI: +64 9 306 8005
Email: jasmine.smart@clendons.co.nz

Clendons
PO Box 1305, Auckland, New Zealand
Phone: +64 9 306 8000
Fax: +64 9 306 8009

Data Matching and Privacy Laws

June 2015

1. Introduction

The collection and commercial use of personal information is a multibillion-dollar industry right now. For example, the 2013 Annual Report for one data-brokering company alone (Acxiom) reveals revenues of $1.1 billion.[1]

Rapid advances in technology have fuelled the collection of vast quantities of personal information by making it not just possible, but also practically viable to collect, share, mine, manage and match information about individuals without their involvement (or even their knowledge).

Recent media revelations have highlighted the fact that personal information isn't just being collected by the websites we visit or our smart phone apps, but also everyday appliances such as TVs: for example, Samsung's SmartTV uses a voice recognition system to collect sounds "including personal or other sensitive information," which is then sent to a third party.[2]

The collection of personal information is often justified under the guise of convenience, and sometimes mistake – although many people now understand that personal information is also being collected for the purposes of targeted advertising.

Facebook offers a tool which allows businesses to exploit their customer information by matching it with Facebook data/ users in order to create a "custom audience" for targeted advertising.

The strike rate or success of an advertising campaign can be massively increased by targeting advertising at consumers with traits / demographics / psychographics / behavioural variables etc more aligned to the advertised subject.

This is where data matching comes in: data matching is a process whereby one set of records / data is compared with another in order to find records in both sets that relate to the same individual. By making that comparison, data matching aims to discover new facts or traits about an individual which, in turn, enables businesses to understand more about their customers– the more information you have, the more you can target your advertising. As a result, data matching and the trading and exploitation of customer databases has now become big business.

The pricing models used in the online performance advertising market are also evolving. Advertisers can now choose whether they adopt a pricing model based on the number of times the advert is displayed (CPM), the number of clicks on the advert (CPC), the number of qualified leads (CPL) or the number of completed actions such as a sale (CPA), amongst others.

Customer databases usually contain personal information, giving rise to important legal issues including:

1. Has the information been collected lawfully; and
2. What are the permitted uses of the information?

It is essential to collect customer / consumer data lawfully, together with consent to use that data as intended. This enables a business to use exciting online and EDM (electronic direct marketing) initiatives in an increasingly mobile world, and subsequently increase the profitability and value of the business.

---

[1] http://www.acxiom.com/wp-content/uploads/2013/09/2013-Annual-Report.pdf
[2] See http://www.stuff.co.nz/technology/gadgets/65985428/samsung-smart-tvs-capturing-and-transmitting-private-conversations

In this Article, we look to discuss the laws surrounding the collection and use of personal information generally, before looking more specifically at the practice of data matching itself.

2. Collecting Information under the Privacy Act

In New Zealand, the collection of personal information is governed by the Privacy Act 1993. The Privacy Act contains a number of "Privacy Principles" which relate to the collection, storage and use of personal information.

In relation to use, the Principles provide (in summary):

(1) The collection of personal information must be for a lawful purpose connected with the function / activity of the business, and must be necessary for that purpose;

(2) The information must be collected directly from the individual concerned, unless:

- The information is publically available;
- The individual concerned has authorised the collection of the information by someone else; or
- The information is anonymous (i.e. not in a form in which the individual concerned can be identified)

(3) Where information is collected directly from the individual, reasonable steps have been taken to ensure that the individual is aware of:

- The fact that information is being collected;
- The purpose for which the information is collected;
- The intended recipients of the information;
- The right to access and correct any personal information held.

(4) Information must not be collected by unlawful means or by means that, in the circumstances, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual;

(5) An individual is entitled to obtain confirmation as to whether or not personal information about them is held, where it is held, and have access to that information.

3. Using Information under the Privacy Act

Information resources can enable competitive advantages. However, little value or competitive advantage can be lawfully obtained from information which cannot be used.

Businesses using unlawfully obtained personal information (in the hope that no one complains) risk investigation by the Privacy Commissioner, referral to the Human Rights Review Tribunal and civil proceedings. Potential liability extends to both employee and employer.

The Privacy Principles provide that:

(1) Before using personal information, the business must have taken reasonable steps to ensure that the information is accurate, complete, relevant and not misleading;

(2) Personal information is not to be held for longer than is required for the purposes for which the information can be lawfully used;

(3) Personal information obtained in connection with one purpose, shall not be used for any other purpose, except in limited circumstances;

(4) Unique identifiers (ie. user IDs) may not be assigned to personal information unless necessary to enable the business to carry out its functions.

The disclosure of personal information is also restricted under the Privacy Principles to a few discrete exceptions, the most fundamental being that the individual has provided consent to that disclosure.

Many aspects of the Privacy Act are now outdated and do not reflect emerging data collection technologies. The practical realities of online advertising, as well as services such as hosting, cloud and disaster recovery, mean that personal data is now being collected by several parties, including services providers that have no direct contact with the consumer, nor the ability to communicate with them.

4. Consent

Under the Privacy Act, individuals may consent to:

- The collection of personal information otherwise than in accordance with the Privacy Principles;
- Personal information being collected from third parties, as opposed to directly from the individual;
- The information being used for purposes other than the purpose for which it was originally collected; and
- The disclosure of the information to third parties.

The obligation to obtain consent prior to the use of personal information is not however limited to the Privacy Act. Obligations requiring consent also arises under:

(a) Confidentiality, both contractual and at common law;

(b) The Unsolicited Electronic Messages Act 2007; and

(c) The Fair Trading Act 1986.

With large scale information collection practices now occurring on a daily basis, businesses need to be vigilant in ensuring that documented, forward thinking consent has been obtained, otherwise the value of the information held may be seriously diminished.

5. Consumer Awareness of Privacy Issues is Increasing

Following public revelations and widespread criticism from privacy advocates in the US, in 2013 Nordstrom ceased use of Elucid Analytics to collect customer data through in-store sensors which track signals from smartphones attempting to connect to Wi-Fi services. Despite assurances from Nordstrom that personal information was not being collected, shoppers seemed unhappy with the revelation that their phones were being used to collect data without their permission.[3]

The New York Times has also reported that "a leading privacy rights group wants the Federal Trade Commission to prohibit Uber from instituting changes to its privacy policy that the group says will allow the ride-hailing app to collect more detailed data about customers' whereabouts and use their contact lists to send their friends promotional pitches."[4]

While individuals have little opportunity to resist the collection of personal information where they require a service (eg. it is necessary to provide your name and other details in order to obtain various services),

[3] http://dfw.cbslocal.com/2013/05/09/nordstrom-no-longer-tracking-customer-smart-phones/
[4] http://www.nytimes.com/2015/06/23/technology/uber-data-collection-changes-should-be-barred-privacy-group-urges.html?hpw&rref=technology&action=click&pgtype=Homepage&module=well-region&region=bottom-well&WT.nav=bottom-well&_r=1

organisations which adopt practices for sharing and collecting information ethically are going to be in a much better position in terms of customer confidence.

6. Data Matching

As a result of rapidly emerging online and EDM (electronic direct marketing) technologies, the number of businesses engaging in data matching is increasing.

Assuming that the customer data held by the business has been lawfully collected, a number of key issues arise, including:

(1) Whether the business is lawfully entitled to share the information with advertising service suppliers or other entities for the purposes of data matching;

(2) The lawfulness of data matching itself; and

(3) Maintaining control of that information.

While the Privacy Act legitimises data matching between specified public sector agencies (provided a number of rules are adhered to) the Act is silent in relation to data matching in the private sector. As a result, data matching in the private sector is, for the most part, regulated by the privacy principles relating to the collection, use and disclosure of personal information, and the use of unique identifiers.

When information is shared between parties, care needs to be taken to ensure the security of the information, and to manage the permitted uses of that information by each party involved. Where a receiving business has not directly obtained consent to collect, hold or use that information, it will be heavily reliant on the terms on which the supplying business obtained the information from its customers.

For example, where information is shared with online advertising suppliers, the business sharing the information needs to make sure that the information:

(a) Is separately identifiable to avoid comingling with other information held by the provider; and

(b) Will not subsequently become available to competitors, or other clients of the advertising provider.

These risks can be managed by ensuring that all steps in the online advertising process, starting with the collection of customer data and culminating in the targeting of advertising to current and prospective customers, take place under appropriate terms and conditions

James Carnie and Jasmine Smart are registered Privacy Professionals with the Office of the Privacy Commissioner.

CLENDONS
BARRISTERS & SOLICITORS

Clendons Barristers and Solicitors
PO Box 1305, Auckland, New Zealand
Phone: +64 9 306 8000

www.clendons.co.nz