

**LAURA RODRIGUEZ RENGIFO**

**ONLINE DATING SERVICES.**

**Emerging consumer law issues.**

**LLM RESEARCH PAPER**

**LAWS 532: CONSUMER LAW**

**FACULTY OF LAW**

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI



**VICTORIA**  
UNIVERSITY OF WELLINGTON

**2015**

*Contents*

I. ABSTRACT .....	<b>3</b>
Word length      3	
II. INTRODUCTION.....	<b>4</b>
III. AN INSIGHT IN THE ODS CURRENT PARADIGM. ....	<b>5</b>
IV. THE ROMANCE SCAMS.....	<b>7</b>
A ODS Users are Vulnerable Consumers: The perfect target for scammers. ....	9
IMAGE 1.....	<b>10</b>
1 The concept of “Vulnerable Consumers” and its implications. ....	11
IMAGE 2.....	<b>14</b>
B Recommendations about how to address Romance Scam And ODS user vulnerability:.....	14
V. ISSUES THAT ARISE FROM THE ODS “TERMS AND CONDITIONS” .....	<b>18</b>
A. ODS Privacy concerns.....	19
B Spam and unwanted messages. ....	27
C Authorizations set up by default, changes and privacy policies and Fair Trade Act.....	28
D . The importance of up to date ODS Privacy Policies. ....	29
VI. CONCLUSIONS .....	<b>30</b>
VII. BIBLIOGRAPHY.....	<b>31</b>
A. PRIMARY SOURCES.....	32
E SECONDARY SOURCES.....	32
VIII. APPENDIX 1. ....	<b>34</b>
IX. APPENDIX 2.....	<b>35</b>
X. APPENDIX 3 .....	<b>36</b>
XI. APPENDIX 4.....	<b>37</b>

## *I. Abstract.*

*Online Dating Service (ODS) has become another medium for individuals experiencing new and creative romantic endeavors with just a few spatial-temporal limits. However, this successful industry is a new target for criminals who look to take financial advantage of ODS users. This type of crime has been identified by media as “Romance Scam”. Additionally, ODS users face the diminishing of their privacy rights when using this services, constant unwanted correspondence, and adverse terms of use. This paper presents an insight on those issues and offer alternatives to address them.*

### ***Word length***

*The text of this paper (excluding abstract, table of contents, footnotes and bibliography) comprises approximately 7023 words.*

### ***Subjects and Topics***

Online Dating Services

Consumer vulnerability

Scams

E-commerce

Privacy Law

Spam

Click-wrap contracts

## II. Introduction.

Online dating services (ODS) have changed the dynamic of human relations, making it easier for individuals to meet people without the need to socialize out of the home. Users who are looking for all kinds of romantic companionship, even marriage, find in OSD a useful tool to meet people around the world that match their expectations. Thus, as the technology and internet evolves, so does ODS , mutating from complex and expensive platforms, to simple and free applications (apps) manageable from mobile devices.

According to the Centre for Law and Justice at Washington, four factors make online dating attractive to customers: anonymity, availability, new form of interactions and making ‘perfect matches’ quickly”<sup>1</sup> . Thus, is expected that the statistics about the number of ODS users will continue to grow massively

There are approximately 1,400 dating sites in North America today, such as Match.com, eHarmony.com, Chemistry.com, and Lavalife.com to name a few “US daters spent approximately \$245 million on online personals and dating services in the first half of 2005.”<sup>2</sup> According to the last report disclosed by the Australian Competition and Consumer Commission (ACC) “industry participants claim membership numbers in Australia in excess of 4.6 million.”<sup>3</sup>

However, the more popular ODS becomes, the larger the number of issues arising from its use. Therefore, ODS are capturing the attention of policy makers, consumer protection bodies and researchers.

---

<sup>1</sup> Fiore, A. & Donath, J “Online Personals: An Overview. ACM Computer-Human Interaction 2004” (July 2004), MIT Media Lab < [http://smg.media.mit.edu/papers/atf/chi2004\\_personals\\_short.pdf](http://smg.media.mit.edu/papers/atf/chi2004_personals_short.pdf)>.

<sup>2</sup> Aunshul Rege “What’s Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud “” *International Journal of Cyber Criminology*. (United States, 2009).

<sup>3</sup> Australian Competition and Consumer Commission. *Online dating industry report* (ACCC 02/15\_927,2015) Retrieved online September 2015 from <https://www.accc.gov.au/publications/online-dating-industry-report>.

The issues that are going to be studied on this paper are: 1. Romance Scams and the vulnerability of ODS users. 2. Privacy issues 3. Spams 4. Default set up terms. Additionally, this paper is going to address some of these issues by giving alternatives of prevention and remedies.

The first segment of this paper contains a general background about ODS and romance scams: how this crime is perpetrated and the modalities that scammers have been using. In the second part, the paper will expose the importance of considering the ODS user as “Vulnerable Consumer”. Thirdly, the paper is going to analyse the most concerning issues that arise from the ODS “terms and condition”. Finally, it will be suggested possible remedies to enforce the current legal frame and address these problems.

### *III. An insight in the ODS current paradigm.*

In this section, the author first describes online dating sites in general, giving an overview of the functionalities that are typically offered by these sites to their users. Today, online dating is an accepted and popular way for people to meet others for companionship purposes. An article on the Journal New Zealand Herald established that “One in five new relationships and one in six marriages is estimated to begin on the net. In the UK, that market now generates 52 million pounds a year and, worldwide, the market size is at least a billion dollars.”<sup>4</sup>

The above numbers are to be expected, since ODS technologic platforms are varied and depend on what the individual is looking for. EliteSingles.com for example, advertise in its site that 67 % of their users are university graduates and over two thirds of their members hold either a Bachelor’s, Master’s or Doctorate degree. This is the feature that aims to make

---

<sup>4</sup> Sarah Rainey “How the world fell in love with online dating” The New Zealand Herald (online ed, Auckland, 24 February, 2015). Retrieved online September, 2015 from <[http://www.nzherald.co.nz/lifestyle/news/article.cfm?c\\_id=6&objectid=11401433](http://www.nzherald.co.nz/lifestyle/news/article.cfm?c_id=6&objectid=11401433) >.

that particular web site different from other ODS and is likely to attract highly educated people. Match. Com is another OSD with similar features to Elitesingles.com. For gaining access to these sites, members need to answer a considerable number of questions and there is also an upfront membership fee, which can be considerable in some cases<sup>5</sup>.

In order to get access to both services mentioned above (Elitesingles.com and Match.com) the future member will have to undergo an extensive questionnaire about personal tastes, beliefs, and private opinions in order to find a match that suits with his or her personality and expectations.

Additionally, users need to upload a few profile photos to reveal their image, which will serve to awaken the appeal of other members. By using advanced search engines and proprietary algorithms, (operating as ‘scientific’ matching services), dating sites instantly find compatible matches based on values, personality styles, attitudes, interests, race, religion, gender, and ZIP codes.<sup>6</sup>

Other example of OSD, which is increasing in popularity, is Tinder. The platform was launched in 2012 and is much more simplistic. This application is accessible from android devices, tablets or iPhones and retrieves the information available in the member’s Facebook profile. Members scroll pictures of other users and swipe right or left depending if their like the photo. Long questionnaires are not required because the focus of this application is judging others by their physical appearance and their zip code.

Regardless the purpose or the portfolio that a particular ODS offers, all of them have the same elements in common: 1) The reason why individuals use them is likely to be the searching for a companionship, which means that probably consumer’s emotions or sentiments are strongly involved during this process. 2) Consumers who sign up with an

---

<sup>5</sup> JingMin Huang, Gianluca Stringhini, and Peng Yong. “Quit Playing Games With My Heart: Understanding Online Dating Scams”. (London, February 2015) University College London <[www.ucl.edu.uk](http://www.ucl.edu.uk)>.

<sup>6</sup> Roy Mitchell “A well-oiled Internet dating machine can generate well in excess of £140 million a year and has replaced the historic personal ad. What is the secret behind one of the Internet’s biggest success stories?” (London, 16 may 2009) Computer world duk <[www.computerworlduk.com](http://www.computerworlduk.com)>.

ODS are encourage to pay money either to enjoy a membership or upgrade the services of the online dating website. 3) Consumers agree with a Terms and Police contract in order to join this websites. 4) Consumers who sign up with an ODS disclosure an important amount of private information to these companies (and third parties) and other ODS users.

These aspects are relevant because they are the most risky characteristics of ODS. As we are going to explore in the next section, criminals have taken all these elements for their advantage to scam victims at alarming rates.

#### *IV. The Romance Scams.*

One issue which is of particular concern for the authorities, among others, is the issue of Romance Scams. “Romance Scams”, or ‘sweetheart swindles’, “are emotionally devastating types of fraud, as scammers make their victims believe they have strong feelings for them.

The romance component of the scam acts as a bait to lure victims, before committing other types of fraud, such as identity theft and financial fraud”. A recent article showed that “in 2014, New Zealanders lost \$1.56 million in online dating scams”. However, loses are not only accountable in money, victims of romance scams receive a “double hit from this crime: the loss of money as well as the loss of a relationship”.

ODS users are considered as a scammer if he/she is using the service to take advantage (mostly economic) of another user<sup>7</sup>. The process of taking advantage of other ODS users by luring them to believe there is potential match is what this paper has presented as “Romance Scam”. Recent reports have revealed that this crime can be a process that can take months<sup>8</sup>, displaying the following elements:

---

<sup>7</sup> Monica Whitty “The Psychology of the Online Dating Romance Scam” (April 2012) The University of Leicester < [www2.le.ac.uk](http://www2.le.ac.uk)>.

<sup>8</sup> Above n 2, at 512.

1. Creating an illusion: scammers elaborate profiles in legitimate on-line dating sites. These profiles are enhanced with characteristics that would lure a large number of victims easily. Some examples are given on the website posted by The Ministry of Business, Innovation & Employment<sup>9</sup> to help consumers to identify scammers. Some “red flags” are “women who are very attractive of mixed ethnicity, around 31 years of age, Christian, looking for a 58-year old male”<sup>10</sup>. All of these fake profiles create an illusion, strategically designed to fit victim’s expectations.
2. Contacting the victim. Scammers then establish a “strong bond with their victims through constant communication to generate confidence, and romantic liaisons”<sup>11</sup>. This stage can take even years, however according to a recent report the time varies depending on each victim. “One victim, for instance, lost approximately £70,000 over a weekend after finding out that the ‘romantic partner’ was a fake after a month”<sup>12</sup>. Some investigations have encountered complex organisations of criminals with sophisticated methods to contact and luring victims by ODS. A report made by CBC exposed that “some networks hired trained psychologists who assisted in further psychologically trapping victims”<sup>13</sup>.
3. Asking for Money. Once scammers have gained the victim’s trust, they ask for money – giving all sorts of excuses. Often, the scammer asks for gifts (e.g., perfume, mobile phone, and laptop) as a testing-the-water strategy<sup>14</sup>. Other times, scammers elaborate a complex story to appeal to the compassionate side of the victim.

---

<sup>9</sup> <<http://www.consumeraffairs.govt.nz/scams/scam-types/dating-and-romance-scams>>

<sup>10</sup> Above.

<sup>11</sup> Aunshul Rege “ What’s love got to do with it? exploring online dating scams and identity fraud”. (2009) Vol 3 (2) IJCC 494 at 512.

<sup>12</sup> Monica Whitty “Anatomy of the Online Dating Romance Scam” (2013) The University of Leicester <[www2.le.ac.uk](http://www2.le.ac.uk)>

<sup>13</sup> Canadian Broadcasting Corporation “Cyber love lost in Russian bride scam” *CBC News* (Online Ed, Montreal, 2008).

<sup>14</sup> Rege, above n 11, at 6.



The online dating romance scam emerged around 2007<sup>15</sup> and it could be considered as an increasing and concerning issue for police-makers, consumer protection agencies and general authorities.

*A ODS Users are Vulnerable Consumers: The perfect target for scammers.*

The ideal paradigm would be for policy-makers and consumers protection agencies to consider ODS users as “Vulnerable Consumers”. *However*, agencies around the world do not give enough significance to the psychologic effects on individuals who use ODS<sup>16</sup>.

*Regarding this point, a research undertaken at The University of Leicester showed that “Little is known about psychological characteristics that may put people at risk of victimization of individual mass-marketing fraud. Even less is known about victims of the romance scam”<sup>17</sup>.*

However, a few studies exposing the psychological aspects of ODS users, have reached important conclusions. First of all, “Loneliness is one of the factors that motivate people to date online, and participants have reported that online relationships reduce their loneliness”<sup>18</sup>. Another aspect reported on a past research showed that users “look for varied, new, complex and intense sensations and experiences and are willing to take physical, social, legal and financial risks for the sake of such experiences”<sup>19</sup>.

All the described factors, contribute to the blurring of the ODS user’s decision-making power. In other words, the vulnerability arises from all the emotions that are involved and can take over the rational thinking of individuals. After all, “Scams, such as lottery scams

---

<sup>15</sup> Rege, above n 11, at 5.

<sup>16</sup> See generally above 3.

<sup>17</sup> Rege, above n 11, at 8.

<sup>18</sup> Lawson, H. M., & Leck “Dynamics of internet dating. Social Science Computer Review” [2006] 24 SSCRS 189 at 208.

<sup>19</sup> Huang, Stringhini, and Peng Yong, above n 8.

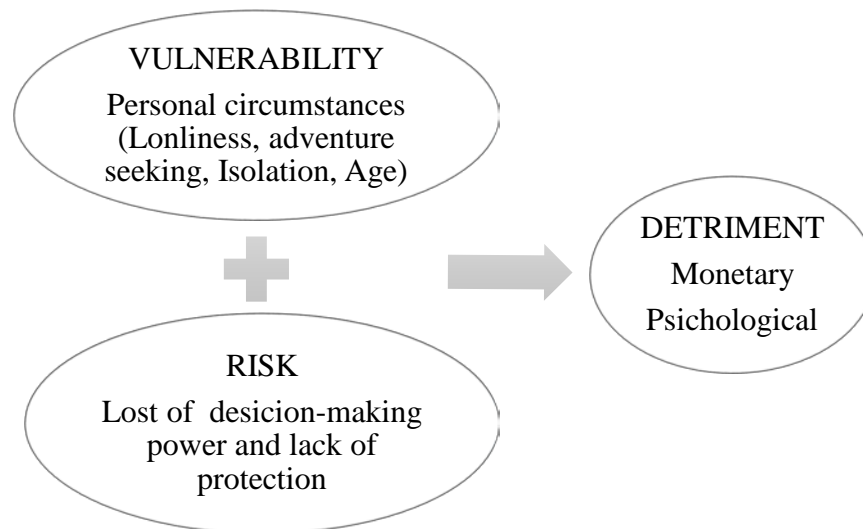
and employment scams, are somewhat less personal, romance scams lower victims' defenses by appealing to their compassionate side"<sup>20</sup>.

The above is consistent with the concept of "Vulnerable Consumer" disclosed on a report written by the Consumer Affairs Victoria:

A person who is capable of suffering detriment in the process of consumption. A susceptibility to detriment may arise from ... the individual's attributes or circumstances which adversely affect consumer decision-making or the pursuit of redress for any detriment suffered.<sup>21</sup>

Another important concept in this study is "the risk" – meaning the probability or likelihood of detriment. As we are going to explore, the risk is amplified by ambiguity in jurisdiction, lack of international collaboration, and consumers' loss of decision-making power.

*Image 1.*



<sup>20</sup> Rege, above n 11, at 6.

<sup>21</sup> Consumer Affairs Victoria *Discussion Paper what do we mean by 'vulnerable' and 'disadvantaged' consumers?* (C-10-01-771, 2004) Retrieved online September 2015 <[www.consumer.vic.gov.au](http://www.consumer.vic.gov.au)>

Lastly, the detriment that vulnerable ODS users suffer from being scammed is not only monetary; the physiological consequences can be devastating as well. They suffered a range of emotional effects including: “shame, embarrassment, shock, anger, worry, stress, fear, depression, suicidal and post-traumatic stress disorder. Some described the feeling of being mentally raped”<sup>22</sup>.

### *1 The concept of “Vulnerable Consumers” and its implications.*

In New Zealand, no statutory law defines the concept of “vulnerable consumer” as a generic premise. Nevertheless, if we examine New Zealand’s sector legislation (rather than generic consumer legislation such as the Fair Trading Act), we can find a number of exceptions, where protection is afforded only to a limited group of consumers, on the basis of their mental, physical or geographical vulnerability.

In the telecommunications sector, section 70 of the Telecommunications Act<sup>23</sup> provides for a “universal telecommunications service”, which ensures that vulnerable consumers of telecommunications services enjoy certain minimum standards of service. Section 70(1) provides:

The purpose of this section is to facilitate the supply of certain telecommunications services to groups of end-users within New Zealand to whom those telecommunications services may not otherwise be supplied on a commercial basis or at a price that is considered by the Minister to be affordable to those groups of end-users.

The obligations arising from this provision are set out in contracts with certain telecommunications operators. For example, the US firm AT&T is contracted to provide a “deaf relay” service to assist people with hearing difficulties to use the telephone system.

---

<sup>22</sup> Whitty, above n6, at 21.

<sup>23</sup> Telecommunications Act 1992 S (70)

The New Zealand firms Spark and Chorus are contracted to provide basic telephone service to geographically remote communities.

In the food sector, the Food Act 2014 provides that

In performing functions or duties, or exercising powers, under this Act (either individually or collectively), the Minister, the chief executive, and all territorial authorities must have regard to the following principles ... (e) the importance of ensuring that regulatory requirements are applied consistently and fairly across sectors and groups in relation to factors such as risk, including, without limitation ... (iii) the intended use of the food, and whether it is intended to be consumed by vulnerable populations.<sup>24</sup>

In the area of drugs, section 4B of the Misuse of Drugs Act requires that, before recommending that the Governor-General make regulations banning a given substance, the Minister must have regard to, amongst other things, “the likelihood or evidence of drug abuse, including such matters as the prevalence of the drug, levels of consumption, drug seizure trends, and the potential appeal to vulnerable populations”.

In the electricity sector, while there has not been any primary or secondary legislation, the Government issued a “Government Policy Statement on Electricity Governance”<sup>25</sup> in May 2009 (the Statement has since been revoked). This led the Electricity Authority to issue its updated “Guideline on arrangements to assist vulnerable consumers” in November 2010. The Guideline “articulates the Electricity Authority’s (Authority) expectations of electricity retailers in respect of vulnerable consumers who may have difficulty paying their electricity bills”<sup>26</sup>.

---

<sup>24</sup> Food Act 2014. S 16.1

<sup>25</sup> Electricity Act 1992.

<sup>26</sup>TCF Disconnection Code Working party, New Zealand Telecommunications Forum. (, Final Paper, March 2013) Retrieved from internet September 2015 < <http://www.tcf.org.nz> >..

Some industries have adopted codes of conduct that aim to protect vulnerable consumers of services in that industry. By way of example, telecommunications operators adopted a “Disconnection Code” in September 2013. Its section “E” requires signatories to “act in a socially responsible manner when dealing with Vulnerable Customers who have identified a need for ongoing Telecommunication Services”<sup>27</sup>.

Additionally, when developing consumer legislation, policy-makers in New Zealand take account of consumer vulnerability. For example, the vulnerability of certain poorer communities to loan-shark services was a factor in the recent “responsible lending” reforms made to the Credit Contracts and Consumer Finance Act 2003. However, these types of consumer legislation are typically framed in a neutral manner, in the sense that they protect “consumers” generally – there is no mention of restricting the protection afforded by the law or regulation to “vulnerable consumers” only<sup>28</sup>.

In markets, generally, some consumers are more vulnerable than others. This may be because they are disabled, mentally unwell, isolated or depressed. “Their vulnerability might be permanent or temporary”<sup>29</sup>.

Concepts like “disadvantage consumer” belong to the area of behavioral economics “which has shown that consumers in a free market do not always act rationally to enter transactions that will maximize their self-interest”<sup>30</sup>. Without going deeper in the behavioral economics theory, it is fair to say that the mental process that leads individuals to make a decision has a high relevance for policy-makers and authorities. Nevertheless, considering ODS users as vulnerable has the following implications (see IV,B).

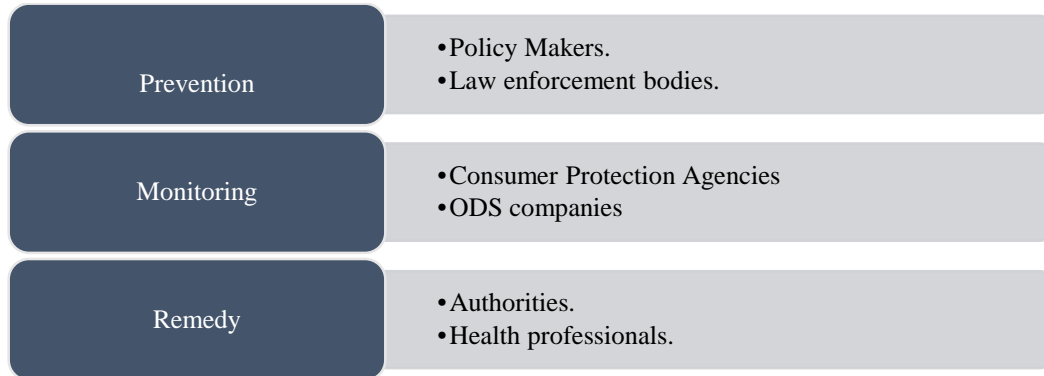
---

<sup>27</sup> The New Zealand Telecommunications Forum Inc. “Disconnection Code”(September, 2013) S 7 <<http://www.tcf.org.nz/>>

<sup>28</sup> Ministry of Consumer Affairs *Consumer Law Reform Additional Paper: Unconscionability* (October, 2010) <[www.consumeraffairs.govt.nz](http://www.consumeraffairs.govt.nz)>

<sup>29</sup> Consumer Affairs Victoria, above 24, at 11.

<sup>30</sup> Kate Tokeley and Others *Consumer Law in New Zealand* (2nd ed, LexisNexis, Wellington, 2014) at 24.

*Image 2.*

Another concept that was explored on this study was the “unconscionability”. This doctrine was discussed by the Ministry of Consumer Affairs in June 2010 on the document “Consumer Law Reform”<sup>31</sup>. This concept was not incorporated on the statutory consumer law reform, and would not apply to ODS users when get scammed. In this regard the Ministry held:

...The reason why the utility of the unconscionability doctrine is limited is that it only applies to the formation of contracts, and it does not apply to the conduct or decisions that a stronger party might make during the course of the contract...Having said that though, the courts are consistently clear that unconscionability is not about rescuing people from the hard or otherwise foolish bargains they might have entered into.

The fact that the unconscionability only apply to the formation of contracts make it futile when it comes to protecting users that have gotten scammed and have been sending money to the offender.

*B Recommendations about how to address Romance Scam And ODS user vulnerability:*

---

<sup>31</sup> Above n 28.

1. Policy-makers: The ideal scenario would be for policy makers to enact statutory laws which coercively engage all ODS industry. The obligations arising from these provisions would be set out in contracts with ODS operators. For example, making mandatory for ODS companies to display scam-warning advertisement on their web site or mobile applications. These advertisements would contain information about how to detect scammers and to guide users on how to protect themselves. Additionally, this law would prescribe a set of minimum digital protection standards in order to avoid identity theft and fake profiles.

Regardless of how effective the above measures could be, the most feasible option in New Zealand would be for policy-makers to publish guidelines<sup>32</sup>. Even if these guidelines are not coercive in nature to engage stakeholders (companies and industry in general, local and international authorities, consumers), they would contribute to an increased level of awareness for ODS users.

The effectiveness of the guidelines would have to be monitored by Law enforcement bodies and authorities. In Australia for example, a report on the results of such guidelines was published in 2015. The Australian Competition and Consumer Commission conducted an Internet sweep which “provided an opportunity to examine the extent to which the guidelines have been adopted and identified opportunities to work further with the industry on disrupting scams, six issues were found after the sweep”<sup>33</sup>.

2. Consumer Protection Agencies and enforcement authorities: First of all, education and information dissemination play a main role in the process of protecting vulnerable consumers. Education creates awareness on the issue and helps to address the ODS issues on preventative basis. In New Zealand, the Ministry of Business, Innovation & Employment has disposed a web site [www.consumeraffairs.gov.nz](http://www.consumeraffairs.gov.nz) to address the most common issues by giving information to the public. However, how much information

---

<sup>32</sup> This is explained by “the current New Zealand Governments principle of “better regulation, less regulation””. Kate Tokeley and Others, above n 29, at 10.

<sup>33</sup> Australian Competition and Consumer Commission, above n3, at 5.

dissemination does this website have? Does the public go to this website before actually using ODS?.

If ODS users were considered vulnerable, authorities would concentrate more efforts to encourage users to visit these informational websites, including Scamwatch.org<sup>34</sup>. Scamwatch.com is a data base of consumer emerging issues, and specially scams. There, consumers are able to find all the reported scams, the modus operandi of criminals, how prevented and how to report it.

The reality is that consumers do not know about these informative tools, and their lack of knowledge about the problem increases the risk of harm. Even more worrying is the attitude towards consumers when they have become victims of scammers already.

When victims do come forward, they are hardly offered assistance from law enforcement agencies. Cukier narrates for example the paradigm in United States:

“While the FBI, US embassies, and local police issue warnings about dating scams, little assistance is offered beyond these admonitions. In some instances, when victims file a complaint with the authorities in countries where the scam originated, they receive a call back from someone claiming to be a police official. This official will then state that their monies have been recovered, but a fee payment is necessary to get the funds back, resulting in yet another scam”<sup>35</sup>

The above shows that victims of romance scams are far from being treated as vulnerable. Otherwise authorities would “provide them with support from health professionals as soon as possible (esp. given that some victims are suicidal when they learn the news). Referrals to health professionals are also necessary given the lack of support from loved ones”<sup>36</sup> .

---

<sup>34</sup>. [www.Scamwatch.org](http://www.Scamwatch.org)

<sup>35</sup> Wendy Cukier and Avner Levin. “Internet Fraud and Cyber Crime. In F. Schmalleger & M.” (Pittaro Ed, New Jersey, 2009) 251 at 302.

<sup>36</sup> Whitty , Above n6 at 20.



3. ODS Companies: Some industries have adopted codes of conduct that aim to protect vulnerable consumers of services in that industry. By way of example, telecommunications operators adopted a “Disconnection Code” in September 2013. Its section “E” requires signatories to “act in a socially responsible manner when dealing with Vulnerable Customers who have identified a need for ongoing Telecommunication Services”<sup>37</sup>. Similarly, some measures to improve the security of ODS users could include “identity proof” or “trusted user” schemes, implemented by other online transactional services such as Trademe or Airbnb. The use of identity validation schemes could greatly enhance the accountability level from the service provider perspective, requiring ODS systems to implement user validation mechanisms while safeguarding the privacy of the data provided by legitimate users. One such measure that is gaining popularity is the use of the RealMe tool, which validates a login trusted profile against a form of identity, such as a driver’s license.

Information on how to spot scammers has to be provided to vulnerable consumers in a more explicit way, in order to catch their attention. Users should be able as well, to report fake profiles even before paying the price of the membership if that is required<sup>38</sup>.

Romantic scams are highly hazardous for unaware ODS users, because the potential harm is not only related to financial losses but also emotional and psychological damage. This type of crime is difficult to address because is perpetrated over the internet and is often cross-border. Authorities acknowledge that they have no jurisdiction in most cases, making user awareness the only plausible way to minimize user’s risk. (See appendix 1)

The question arising from the above is: if it is problematic to give a remedy to victims of scammers, would there be a better solution to improve on the prevention side of the issue?

---

<sup>37</sup> Above n 26.

<sup>38</sup> Australian Competition and Consumer Commission, *above n3*.

Another point regarding this is that current prevention mechanisms may not work effectively if policy makers and authorities do not consider ODS users as vulnerable consumers; which makes the problem difficult to address from a legal standpoint.

V. *Issues that arise from the ODS “Terms and Conditions”.*

“Terms and Conditions” is an agreement or electronic contract that establishes the legally binding terms ODS users must accept in order to use the Service. This agreement includes most of the times, the Privacy Policy, terms about safe use, pricing, purchasing or accepting of additional features, governing features, billing, free trials, discounts and promotions.

Websites and applications dispose these terms and conditions in form of “wrap contracts”<sup>39</sup>. The user agrees with all the content of the contract by giving a click on an “acceptance box” and pressing send. This kind of contract is a new form of agreement used in electronic trades and has been object of discussion on the case law and the doctrine.

Although it has been accepted as a valid method to incorporate terms<sup>40</sup> in the case of ODS agreements its lawfulness is debatable. The information that users disclose to ODS companies could be extremely personal and sensitive, and the question that arises is if “wrap contracts” is a method that protects consumers, or is more a tool for business like ODS companies to breach users privacy rights.

Additionally, a paramount problem on this study is, under what law or jurisdiction these terms are written? Mostly the jurisdiction that govern ODS activity is a set up on the “terms and conditions” agreement. This led us to explore deeper which websites or apps are used on the market at New Zealand, and by which jurisdiction they are ruled.

For the purpose of this study the website [www.nzdatingwebsites.co.nz](http://www.nzdatingwebsites.co.nz) was used to identify the ODS most popular at New Zealand (see appendix 2). With the information this website

---

<sup>39</sup> See more at Kate Tokeley, above n 29, at 489

<sup>40</sup> at 489.

provides, is feasible to group ODS in three big categories depending on what jurisdiction governs their activity:

- a. Websites that directly claim being under New Zealand jurisdictions: Nzdating.com and Findsomeone.com for instance, are New Zealand made or operated and additionally they set up on their contracts that the applicable jurisdiction is from New Zealand (see appendix 3).
- b. Others like Match.com.nz despite having an online address that suggest to consumers that is a New Zealand “made”, is actually based on United States and its terms set up that jurisdiction as applicable. Another example is Eltesingles.com.nz that is based in Germany.
- c. ODS that explicitly and exhaustively claim to be governed by other jurisdictions outside of New Zealand. Tinder for example established on its “Terms and Condition” agreement:

This Agreement, and any dispute between you and the Company, shall be governed by the laws of the state of Texas without regard to principles of conflicts of law, provided that this arbitration agreement shall be governed by the Federal Arbitration Act<sup>41</sup>.

The above classification is going to be useful on the next title. This paper is going to explore the privacy issues that arise from the terms and conditions agreements, based on the jurisdiction they are governed for.

### ***A. Privacy concerns.***

As this paper has shown, ODS users are in potentially vulnerable because of their psychological and emotional state. To this end, it must to be added that they disclose not only financial information when using ODS, but sensitive data as well. The nature of the service we are studying is closely connected with the most intimate aspects of individuals, therefore the data they share is not public and has to be protected.

---

<sup>41</sup> Tinder “Terms and Conditions agreement” <[www.gotinder.com](http://www.gotinder.com)>

ODS companies' collect all types of data about users', financial and personal information. Personal information for instance is collected by ODS companies through questionnaires, quizzes, and pictures. All this information is disclosed by users, often to allow ODS to apply algorithms that match them with compatible individuals.

The information that users disclose has to do with their religion, sexual preferences, political and philosophical association and even with their health. There is not a wide range of services on the internet capable of obtain such insight on consumers' data. But the heart of the matter is not all the private information ODS<sup>42</sup> companies are able to collect by questionnaires and other methods, but the intention of the users to disclose this data. Users give their most personal information to ODS companies with the solely purpose to match them with compatible partners.

It could be argued that a large number of Facebook users share personal information on their pages as well, but they do that with the purpose of making it public. Whereas, ODS users are giving the information to the ODS company believing that it is going to be protected and used mostly to find them companionship.

Additionally, this information related with the intimate core of the individual (sexual orientation, religion, health issues, and etcetera) has been the object of international protection<sup>43</sup> under the classification of "sensitive data". "The large majority of the actual laws may certainly suggest that the attribute "sensitive" is reserved to an exclusive class of data carefully selected by the legislators"<sup>44</sup>.

---

<sup>42</sup> An ODS company fits on the definition of an "agency". An "agency" is almost everyone who holds personal information under the Privacy Act s 2.

<sup>43</sup> "Art. 8 of the Data Protection Directive (95/46/EC), of the Directive contains a general prohibition on processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Other than the categories "ethnic origin", "philosophical beliefs", "trade-union membership" and data concerning criminal convictions". The Data Protection Directive 95/46/EC of the United Nations.

<sup>44</sup> Spiros Simitis "Revisiting Sensitive Data" (April, 1999) Johann Wolfgang Goethe University of Frankfurt am Main <[www.coe.int](http://www.coe.int)>

Although, The New Zealand Privacy Act does not have a 'sensitive categories' of information “the Human Rights Act 1993 and the New Zealand Bill of Rights Act 1990 outlaw discrimination in a range of circumstances. These grounds would encompass most found in a typical list of 'sensitive categories' with some additional ones.”<sup>45</sup>

On the other hand, Australia has defined this category of information under the Australian Privacy Act 1988 as following:

Means information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or membership of a trade union, sexual orientation or practices, or criminal record that is also personal information or health information about an individual, or genetic information about an individual that is not otherwise health information, or biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates.

As is seen from these definitions, is fair to say that often ODS companies have the custody of sensitive information. All the matters related to this data are set up in their “Privacy Agreements”. Those agreements are accepted by users with the aggravating circumstance that ODS companies use “Click-wrap” methods as was explained in the past title.

This is a disadvantageous situation for ODS users, because firstly, users often accept the terms of privacy without reading. Alan Toy explained this issue:

Authorization should be interpreted in a way that ensures users of websites are fully able to understand and manage their rights to information privacy in the

---

<sup>45</sup> Privacy Commissioner to the Minister of Justice “Electronic Commerce: Part 2 - A Basic Legal Framework” (Law Commission, November 1999) < <https://www.privacy.org.nz>>

online context... It may be difficult to enforce such an agreement as a contract, especially where the link to the policy is not obvious to a user of the site <sup>46</sup>.

Additionally, the applicable law is not always effective at protecting consumer privacy in cyber-space. As was shown in the past title of this paper, ODS companies that are based in New Zealand are required to meet the provisions of the New Zealand Privacy Act. However, apps like Tinder are not governed by New Zealand jurisdiction in this respect (see Title V).

To illustrate this point see the next table where a comparison between a ODS based in New Zealand, FindSomeone.com, and Tinder is shown. A conclusion of this comparison is that Tinder and FindSomeone.com define the information they collect as “personal information” and “financial information”. Additionally, none of them define the data they hold as “sensitive information”.

<b>Differences between the treatment of information between</b>	<b>Tinder<sup>47</sup>.</b>	<b>Findsomeone.com<sup>48</sup> operated by Trademe.com</b>
What kind of information they collect.	Facebook account information, such as public Facebook profile (your email address, interests, likes, gender, birthday, education history, relationship interests, current city, photos, personal description, friend list, and information about and photos.	Is not very clear what is the exactly the information THIS ODS collect. Among others: Financial information such as the credit card number. Demographics, interests, and behavior, localization, address, email, mobile, photos.

<sup>46</sup> Alan Toy “Consent to Online Privacy Policies” (2009) 15 NZBLQ 236 retrieved from <www.westlaw.com>

<sup>47</sup> Above n 38.

<sup>48</sup> Privacy Policy <www.findsomeone.nz.co>

<p>How they collect the “personal information”.</p>	<p>When users upload photos, a personal description and information about gender and preferences for recommendations, such as search distance, age range and gender. If the user chats with other Tinder users, they provide Tinder the content of your chats.</p> <p>Contact us with a customer service or other inquiry</p>	<p>Questionnaires, messages with help desk, activity and links that the user give click in while using the site.</p> <p>When the user fill the questioner.</p>
<p>Who ODS share information with?</p>	<p>“he Match Group’s businesses include the online dating websites and apps Match.com, OkCupid, OurTime.com, BlackPeopleMeet.com, Twoo, Meetic, HowAboutWe and others.”</p> <p>They Also set out:</p> <p>“In connection with a substantial corporate transaction, such as the sale of our business, a divestiture, merger, consolidation, or asset sale, or in the unlikely event of bankruptcy.”</p>	<p>This ODS claim that will never sold to any other party and will never be disclosed Users information without their permission.”.</p>
<p>Applicable Jurisdiction</p>	<p>Laws of the state of Texas without regard to principles</p>	<p>New Zealand Privacy Act</p>

	of conflicts of law, provided that this arbitration agreement shall be governed by the Federal Arbitration Act.	
--	---	--

Although, in order to collect information in New Zealand, it is not mandatory for ODS classify the information as sensitive, it begets the question if in other jurisdictions like Australia or European Union (whose privacy laws contain the “sensitive information” category) authorities would be able to require the inclusion of this term.

Another outcome of the analysis of these websites privacy terms was that Findsomeone.com does not meet the requirements of the Privacy Act<sup>49</sup>. One example of this is given in the cl 7 where the privacy policy<sup>50</sup> set out:

...FindSomeone will not access your information from Facebook without your express permission. However, when you grant permission you are authorising FindSomeone to collect, store, retain and use indefinitely, any and all information that you agreed Facebook could provide to FindSomeone through the Facebook application programming interface.

Regardless of that Principle 9 of the Privacy Act provides that the company should not retain personal information for longer than is necessary. The above term establishes that users are giving the permission to the ODS company to use indefinitely all the Facebook information. The perennial use of the Facebook information by the ODS company is not explained on the agreement body.

---

<sup>49</sup> Privacy Act, S 23.

<sup>50</sup> FindSomeone.com Privacy Policy <[www.finsomeone.com.nz](http://www.finsomeone.com.nz)>



There are many exceptions where the Principles do not apply<sup>51</sup>, however Principle 9 has no exceptions even if “there are no set time frames attached to this principle”<sup>52</sup>. On the other hand, the app Tinder, is even more unfriendly with the user. Its privacy provisions are set out in its cl 7<sup>53</sup>:

... The Match Group’s businesses include the online dating websites and apps Match.com, OkCupid, OurTime.com, BlackPeopleMeet.com, Twoo, Meetic, HowAboutWe and others. We may share information we collect, including your profile and personal information such as your name and contact information, photos, interests, activities and transactions on our Service with other Match Group companies.

Despite that, Tinder is not governed by the Privacy Act, it does not specify why or with what purpose the information is going to be shared. The information that Tinder collected is basically all the data users upload to Facebook. This causes another problem, because even if users close their Facebook account, Match Group will still having all their information. Privacy Rights Clearinghouse <sup>54</sup> notes regarding the above:

... Once an online dating service has your information, it has it for keeps. Even after you cancel your account (fall in love, get married, take a vow of celibacy, etc.), most dating sites retain your information...

Another troublesome matter, is the sharing itself of such sensitive information between companies of the same group. Elitesingles.com for example sets out at the beginning of the Privacy Policy agreement:

---

<sup>51</sup> Privacy Act, S 6, Privacy Principles 3,10, 11.

<sup>52</sup> Kate Tokeley, Above n 29, at 492.

<sup>53</sup> Tinder Privacy Policy <[www.gotinder.com](http://www.gotinder.com)>

<sup>54</sup> Privacy Rights Clearinghouse “Fact Sheet 37: The Perils and Pitfalls of Online Dating: How to Protect Yourself” (March, 2015) <[www..privacyrights.org](http://www.privacyrights.org)>

..Personal information will only be passed on to third parties if necessary to provide the service offered (e.g. payment processing for fee-based memberships)...

This clause, makes the users believe that their personal information won't be shared unless it has to do with the service. However, at the end of the contract there is another provision that established:

We reserve the right to transfer any personal information we have about you in the event that we sell or transfer all or a portion of our business or assets to a third party...<sup>55</sup>

In this regard, the Fair Trading Act 1986 may apply because the privacy policy contradict itself and can mislead the user. Furthermore, the right to transfer personal information when they sell a portion of their business, is set up as default ( See IV, C). Alan toy, notes in this regard:

The Fair Trading act may apply...where a privacy policy states that personal information will not be sold to third parties without the consent of the user, it could be considered misleading or deceptive to divulge it in a way contrary to such a statement... This is especially important where the website operator has collected information for one purpose but now wishes to use it for another...In such cases, best practice is for the website operator to seek fresh consent from users.<sup>56</sup>

United States case law had a similar approach to this issue for example in *Feldman v Google* <sup>57</sup>., the District Court decided the terms of the agreement were displayed in

---

<sup>55</sup> Elitesingles.com Privacy Policy <<https://www.elitesingles.ca/en/privacy>>

<sup>56</sup> Alan Toy, above n 42, at 3.

<sup>57</sup> *Feldman v Google Inc* 513 F Supp 2d 229, at p 236 (2007 US District Court for the Eastern District of Pennsylvania).

a box on a website, but not all of the terms were visible without scrolling down the website page.

In other words, sharing personal information of users should not be set up on the privacy policy by default but instead a new authorization should be sought when needed. Secondly, it could be considered as misleading the practice of having privacy policies that contradict itself in order to confuse users and make them believe that their personal information won't be shared.

*B Spam and unwanted messages.*

One of the ODS companies, NZDating.com, set up on its Privacy Policy agreement:

...Our site provides users the opportunity to opt out of receiving communications from NZDating. NZDating gives users the following options for removing their information from our database to not receive future communications or to no longer receive our service. However we do also have mandatory newsletters for our members and the only unsubscribe option is to remove your membership from NZDating...<sup>58</sup>

As is observed from the transcription of these click wrap terms, there are “mandatory newsletters” that have no unsubscribe option other than renouncing to the service itself. Additionally, it does not specify what the purpose of these newsletters is.

If that clause is analyzed at the light of the Unsolicited Electronic Messages Act 2007 it is feasible to say that it is breaching consumers' rights. According to the Act agencies must provide a “functional unsubscribe facility”<sup>59</sup> on their electronic messages and this disposition has no exceptions.

---

<sup>58</sup> NZDating.com Privacy Policy <[www.nzdating.com](http://www.nzdating.com)>

<sup>59</sup> Unsolicited Electronic Messages Act, s 11.

However, through the clause outlined above, NZDating.com withdraw the right of users to unsubscribe from receiving messages. Therefore, the question that arises is whether this kind of mandatory communication, attached to the use of the service, is detrimental to the right of unsubscribe. Note that this authorization is set up by default as this paper is going to explore in the next title.

*C Authorizations set up by default, changes and privacy policies and Fair Trade Act.*

Is a Common practice for ODS companies to established default settings about privacy. For instance Match.com set up in its privacy policy agreement:

...Most browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies. If you choose to decline cookies, please note that you may not be able to sign in or use some of the interactive features offered on our website...

Cookies is a technology that tracks users' preferences by registering all their online activity. The above clause highlights how this preference is set up by default. Best practice for ODS companies is to set up cookies as an explicit preference and not by default. In this regard Alan Toy notes:

Further dangers are raised by the use of default options in online policies. Default options can be used by website operators to encourage consumers to assent to certain uses of their information. For example, there might be a pre-ticked box allowing the website to use the contact details of the consumer for marketing purposes (cookies)...<sup>60</sup>

Alan Toy wrote the above, under the title of 'irrational behavior' of consumers. It means that individuals are prone to make detrimental choices for their rights and sometimes are

---

<sup>60</sup> Alan Toy, n 42, at 10

overoptimistic about consequences. “Users of websites are more likely to retain the status quo rather than the alternative”<sup>61</sup> even if the alternative is better for them.

***D . The importance of up to date Privacy Policies.***

As was mentioned before, the best practice for ODS companies would be seek explicit authorization of users, each time that privacy policies change. However, some ODS companies like NZDating.com establish terms as the following:

These terms and conditions may be updated from time to time, without notification. You are responsible for ensuring you are familiar with the latest terms and conditions and privacy policy, the last update was 1 July 2010<sup>62</sup>

As was presented above, NZDating.com make mandatory for users receiving e-mails and communications. However, this company transfer the responsibility to the user for being familiar with the latest terms and conditions.

In this case, is feasible to conclude that The Fair Trade Act is applicable. First of all, because the agreement allow to the ODS company change privacy conditions unilaterally. The Commerce Commission expressed in this respect:

Many of the examples are of terms that allow a business to make changes to the contract or to what they are supplying, without an equivalent right being provided to the other party<sup>63</sup>

---

<sup>61</sup>At 10.

<sup>62</sup> <http://www.nzdating.com/general/terms.aspx>

<sup>63</sup> Commerce Commission *Unfair Terms Guideline* (February, 2015) < [www.comcom.govt.nz](http://www.comcom.govt.nz) >

Secondly, because it is the responsibility of the ODS company to maintain terms up to date, and as is seen from the clause the last update was five years ago. In this regard Alan Toy express: “Other misleading and deceptive conduct could stem from having a privacy policy that is not up to date”.

## *VI. Conclusions*

This paper has shown that ODS users are potentially “vulnerable consumers”, given the transactional nature of ODS service provision and the minimum online protection measures expected from a web-based, service-client perspective.

This study has also explored, the specific characteristics of the match-making market, especially the type of consumer who may be vulnerable to scams (the lonely who may feel a social pressure to find a relationship, or people with low levels of self-esteem). When such people “fall in love” with a match, their vulnerability increases (love has been equated by some researchers to a mental state of illness or obsessive compulsive disorder).

In addition to vulnerability, we explored the concept of “the risk” that represents a possibility of harm. The risk is increased by the lack of protection of these types of consumers and the poor regulation of ODS industry. The non-existence of cooperation between countries and the difficulty associated with protecting the activities of individuals over the internet further increases the risk of harm to users.

If policy-makers and authorities do not strengthen protection measures against this particular type of cybercrime, consumers will continue to be easily targeted by online scammers, which operate without any concerns given the lack of legal support offered to legitimate ODS users.

In addition to scammers, the ODS industry is not “consumer friendly” either. This paper presented some actual facts about the “terms and policies”, agreements that should catch

the attention of authorities. ODS companies are imposing terms on users that might be detrimental to their privacy rights without any penalty.

It is fair to say that in New Zealand, the ODS industry is taking advantage of flaws on the legal system, such as: 1. Limitation of jurisdiction in cross border issues 2. Laws about electronic commerce and privacy rights are stagnant and do not take into account new forms of contracts like “click-wrap” 3. ODS Companies set up authorizations by default instead of looking for an explicit consent from the user without any restriction.

The issues that arise from “terms and conditions” and “privacy policies”, also have to do with a hierarchy of the applicable law. It is a common belief that those agreements are entirely governed by contract law, whereas in reality “freedom of contract” is restricted by privacy law. In this regard Alan Toy notes: “Freedom of contract is justifiably limited by consumer protection legislation such as the Privacy Act 1993.”<sup>64</sup>

To raise awareness about the importance of developing “terms and conditions” agreements under the consumer law instead of contract law, policy-makers must disclose guidelines. In New Zealand for instance, the Ministry of Business and Innovation shall engage the ODS industry through guidelines of “best practice”. It is recommendable for Law Enforcement Agencies to conduct a swap over the internet and monitor the “terms and conditions” agreements, before and after these kind of guides are released.

Among the issues described in this paper, it opens the discussion about the match making market and its regulations regarding other aspects. For instance, misleading advertising, the auto-renewal practice, educational campaigns and the protection of children.

## VII. *BIBLIOGRAPHY*

---

<sup>64</sup> Alan toy, above n 42.

**A. PRIMARY SOURCES.**

## LEGISLATION

Weights and Measures Act 1987.

Consumer Guarantees Act 1993.

Fair Trading Act 1986.

Food Act 2014.

The Electricity Act 1992.

Telecommunications Act 2013.

Unsolicited Electronic Messages Act.

## INTERNATIONAL MATERIAL

United Nations The Data Protection Directive 95/46/EC .

**E SECONDARY SOURCES**

## BOOKS AND CHAPTERS IN BOOKS.

Kate Tokeley and Others *Consumer Law in New Zealand* (2nd ed, LexisNexis, Wellington, 2014)

Matthew Williams *Virtually criminal : crime, deviance, and regulation online* (Routledge, New York, 2006)

Ernesto Ugo Savona *Crime and technology : new frontiers for regulation, law enforcement and research* (Springer, Italy, 2006 ).

Leonard Reinecke *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Springer Berlin 2011)



Gary Bahadur *Privacy Defended: Protecting Yourself Online* (Que, Berlin, 2002)

#### JOURNAL ARTICLES

Sally Blundell “The elderly are at the mercy of new scams and shameless family members”  
TLM (Online ed, New Zealand, 12 September, 2014).

Aunshul Rege “What’s Love Got to Do with It? Exploring Online Dating Scams and  
Identity Fraud” *International Journal of Cyber Criminology*. (United States, 2009).

Nicole Ellison “Managing Impressions Online: Self-Presentation Processes in the Online  
Dating Environment”. (2006) *JCC* 11.2 415-441

Alan Toy “Consent to Online Privacy Policies” (2009) 15 *NZBLQ* 236 [www.westlaw.com](http://www.westlaw.com)

#### REPORTS

Australian Competition and Consumer Commission. Online dating industry report (ACCC  
02/15\_927,2015)

#### INTERNET RESOURCES.

Andrew T. Fiore and Judith S. Donath “Online Personals: An Overview. *ACM Computer-  
Human Interaction* 2004” (July 2004).

Wendy Cukier and Avner Levin. “Internet Fraud and Cyber Crime. In F. Schmallegger &  
M.” (Pittaro Ed, New Jersey, 2009) 251 at 302.

Arms, S “Romance Scam: Scammers Feign Affection to Commit Fraud”( April 2010)

Monica T. Whitty “The Online Romance Scam: A Serious Cybercrime“ (February 2012)  
The University of Leicester < [www2.le.ac.uk](http://www2.le.ac.uk)>.

Monica Whitty “The Psychology of the Online Dating Romance Scam” (April 2012) The  
University of Leicester < [www2.le.ac.uk](http://www2.le.ac.uk)>.

Ministry of Consumer Affairs Consumer Law Reform Additional Paper: Unconscionability  
(October, 2010) <[www.consumeraffairs.govt.nz](http://www.consumeraffairs.govt.nz)>

JingMin Huang, Gianluca Stringhini, and Peng Yong. “Quit Playing Games With My  
Heart: Understanding Online Dating Scams”. (London, February 2015) University College  
London <[www.ucl.edu.uk](http://www.ucl.edu.uk)>.

ABA International Guide to Combating Cybercrime

Elitesingles.com Privacy Policy

FindSomeone.com Privacy Policy

### *VIII. Appendix 1.*

The following is a screenshot of the Consumer affairs web site designed by The Ministry  
of Business and Innovation to help consumers. As is seen from the image the main message  
that the Ministry communicate is “New Zealand law is unlikely to be able to help you”<sup>65</sup>.

---

<sup>65</sup> [www.consumeraffairs.govt.nz](http://www.consumeraffairs.govt.nz)

www.consumeraffairs.govt.nz/scams/been-scammed

Global Shop SV TORTIOUSLY meani... Office 365 translate - Google S... Drag to Reposition ... Music for everyone ... you tube Netflix ebrary ProQuest Re...

I bought suspicious medicine

Protect others

It's very important to act as quickly as possible, before it is too late.

### In New Zealand

If the scam originates in New Zealand you may be able to get help under New Zealand law. In this case, the Ministry of Consumer Affairs advises you to:

- Contact the Police to lay a complaint, as the scam may be illegal – and the scammers may be criminals who can be found and prosecuted.
- Talk to your Citizens' Advice Bureau to get independent, impartial advice about what else you can do and where you may be able to go to get help or redress.

### Overseas scam

If the scam originated overseas, New Zealand law is unlikely to be able to help you.

If you have sent money there is very little chance of getting it back.

You can follow up with the relevant Authority of the area from which the scam originated. You can find a list of Authorities and their jurisdictions at the International Consumer Protection and Enforcement Network.

➤ [Visit the ICPEN website.](#)

You can also help to protect others from the scammers that have taken you in or tried to take you in. You can report the scam through our Protect Others section and we may publish information about it on our Alerts section, without revealing your identity.

[Protect others from being scammed.](#)

[Immigration New Zealand has been made aware of a new scam website which appears to be a direct copy of the home page of the official Immigration New Zealand website, with a slight change in the domain name.](#)

24 June 2015 - Scam Alert - Small Business Scam  
[New Zealand small businesses are being targeted in a scam originating from a German company.](#)

19 May 2015 - Scam Alert - Immigration Scam  
[Indian nationals living in New Zealand are being targeted by a new wave of scam phone calls claiming to be from Immigration New Zealand.](#)

5 December 2014 - Scam Alert - Facebook beware  
[The risks involved when you buy through Facebook.](#)

16 October 2014 - Spark New Zealand scam  
[Spark customers targeted by ongoing fraudulent phone calls.](#)

Last updated 20 May 2010 [^ Top](#)

[Site map](#) [Privacy and copyright statement](#) [Disclaimer](#) [Contact us](#) [Social media policy](#)

newzealand.govt.nz

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT  
HĪKINA WHAKATUTUKI

Copyright © 2010. All rights reserved.

## IX. Appendix 2.

The following, is a list of the top online dating sites built by Sheldon Nesdale and disposed on NZDatingWebsites.co.nz. According to online journal, Stuff .co, this is a complete list of the ODS available in New Zealand<sup>66</sup>.

<sup>66</sup> Richard Medow “True love at a price” Stuff.com (Online ed, Auckland, 10 October 2013)  
<<http://www.stuff.co.nz>>

Websites	Apps
1. www.EliteSingles.co.nz 2. www.FindSomeone.co.nz [Built by TradeMe] 3. www.DatingBuzz.co.nz 4. www.FlirtBox.co.nz 5. Match.nz.msn.com / Dating.nz.msn.com 6. www.SinglesClub.co.nz 7. www.NZPersonals.com 8. www.NZ.Match.com 9. www.HaveAFling.co.nz 10. www.DatingNZSingles.co.nz 11. TwoSome.co.nz 12. www.ZingleBook.co.nz	1. Tinder: www.GoTinder.com 2. Fancied: www.GetFancied.com Play 3. EHarmony: www.eharmony.com/mobile-dating-app/ <input type="checkbox"/> Apple iTunes 4. Pozee: www.pozeeapp.com <input type="checkbox"/> 5. New-Zealand.SinglesAroundMe.com 6. Christian Mingle: www.christianmingle.com/mobile 7. Hinge: hinge.co 8. We Are Her: weareher.com [Lesbian] 9. rindr: grindr.com [Gay Men] 10. Scruff: scruff.com [Gay Men] 11. Skout: www.skout.com 12. Happn: www.happn.fr/en/ 13. Bumble: bumble.com 14. EliteSingles.co.nz

### X. Appendix 3


The following is a screenshot of the website www.NZDating.com where they claim to be “100% NZ owned and operated”.

- The ability to store and display up to four photos
- Priority over other free members in the search results
- Silver Member Star in Profile and Listings
- Access to members profiles that don't allow members with free email
- [Read More about a free Silver Membership...](#)

**Gold Membership gives you:**

- Top listings in search results
- Access to 'Buddy' lists to control photos and messaging
- The ability to store and display up to twenty photos
- Gold Member Star and highlighting in messages, profile and listings
- Access to members profiles that only allow paid member access
- Priority Support
- [Read More about Gold Membership...](#)

---



**NZDating is 100% NZ owned and operated**

NZDating is one of very few online dating services that is truly 100% NZ owned & managed, ensuring our focus is on developing the very best service specifically for Kiwis!

<b>Friendship and Dating in New Zealand</b>			<b>Explore NZDating</b>		
Auckland	Bay of Plenty	Canterbury	Join Free!		
Gisborne	Hawkes Bay	Horowhenua	HOME		
Manawatu	Marlborough	Nelson & Bays	Success Stories		
Northland	Otago	Southland	New to NZDating?		
Taranaki	Timaru & Oamaru	Waikato	Need Help?		
Wairarapa	Wellington	Wanganui	What's New		
West Coast			Who's Online?		
<a href="#">Help</a> • <a href="#">Terms of Use</a> • <a href="#">Your Safety</a> • <a href="#">Your Wellbeing</a> • <a href="#">Contact Us</a> • <a href="#">Testimonials</a> • <a href="#">Your Privacy</a>					

©2015 NZDating.com

## XI. Appendix 4.

The following is the transcription of “Privacy Statement” disclosed by NZDating.com and available on their website: <http://www.nzdating.com> general > See privacy.aspx>

NZDating has created this privacy statement in order to demonstrate our firm commitment to our members privacy. The following discloses our information gathering and dissemination practices for the NZDating website. Please note this statement is as at 3 January 2008. NZDating is always evolving and will endeavour to remain within the bounds of this statement or keep this statement current. NZDating will always endeavour to comply with the conditions of the New Zealand Privacy Act.

In the case of known or suspected abuse of our systems or members, we reserve the right to review and pass any relevant information stored on our systems to the relevant ISP(s) or Police to help prevent the abuse, we will also provide assistance to help identify a member

for members who are proceeding with in our view legitimate legal action. We feel the protection of our members is one of our most important goals.

### **Data Collection**

- IP Address - We use your IP address to help diagnose problems with our server, and to administer our Web site. Your IP address is also used to help gather broad demographic information that is not tied back to you personally.
- Cookies - Our site uses cookies as for logins and for keeping options specific to a browser.
- Personal Details - As a dating and freindship website we ask our members for a number of personal details for use on the website. We always try to identify which information is for system use and which is for displaying to other members.
- Email Address - The email address provided will only be used by NZDating for notification events, contacting the member ourselves and newsletters. It will not be sold for other purposes or given to other members. Where possible opt out options may exist for notifications and newsletters, however some newsletters are not optional and you will need to remove your NZDating membership to unsubscribe.
- Demographic Data - Demographic and profile data is also collected at this site. We use this data to tailor the visitor's experience at this site, showing them customised content we think they might be interested in, and displaying the content according to their preferences. We also employ the services of Netratings and Google Analytics to independently verify the number of visitors and other basic demographic information on our site.
- Advertisers - From time to time we summarise demographics and other details, such as the number of members under 30, any information is shared with advertisers on an aggregate basis only.

### **Other Web Sites**

This site contains links to other sites. NZDating is not responsible for the privacy practices or the content of such Web sites.

### **Orders and Membership signup**

Parts of our site may use an order form for customers to request information, products, and services. We collect visitor's contact information (like their email address) and financial

information (like their account or credit card numbers). Contact information from the order form is used to send orders, and provide information about our company. The customer's contact information is also used to get in touch with the visitor when necessary. Any financial information that is collected is used to bill the user for products and services.

### **Optional Surveys**

From time to time we may run optional online surveys in which we may ask visitors for additional contact information and demographic information. We use contact data from our surveys to send the user information about our company and promotional material from some of our partners. In such surveys users may opt out of receiving future mailings.

### **Competitions and Promotions**

We may run promotions on our site in which we ask visitors for contact information. We may use contact data from our contests to send users information about our company and promotional material from some of our partners. The customer's contact information is also used to contact the visitor when necessary, usually for prize delivery. Users may opt out of receiving future mailings; see the choice/opt-out section below.

### **Banner Advertising**

We use an external ad Web site to display ads on our site. These ads may contain cookies. While we use cookies in other parts of our Web site, cookies received with banner ads are collected by our ad company and are only used for ad tracking. We may pass coded information to the ad server in order to target banners based on our member's settings.

### **Public Forums**

This site makes chat rooms, forums, message boards, and/or news groups available to its users. Please remember that any information that is disclosed in these areas becomes public information and you should exercise caution when deciding to disclose your personal information. You should assume that all chat rooms, forums and message boards are logged for historical or monitoring purposes and may be summarised and displayed.

### **Internal Email System**

Messages using our internal email system are not able read by any other members other than the sender and receiver. Once a message is sent it is not possible to retract it. Some membership options may allow a sender of an email to see when their sent email was read

or if it was deleted. NZDating have a number of security filters and procedures that are run over internal email to prevent site abuse, commercial use and spam. As part of these processes from time to time NZDating staff may be required to view messages, however they will always remain private and confidential, the only time these messages will be disclosed to any other party is if the member is involved in legal proceedings and either NZDating is satisfied that the legal action is justified, or the disclosure is a legal requirement.

### **Member Profiles, Adverts and Photos**

NZDating have a number of security filters and procedures that are run over member profiles and photos to help prevent site misuse, unauthorised commercial use and spam. As part of these processes from time to time authorised NZDating staff may be required to view member profiles, adverts and associated material.

### **Shared Member Information**

As a core function of NZDating, various elements of your profile, the last time you have been on the NZDating website, and other statistical information may also be available to members such as ratios on how often you reply, block, use messageboard hammers and other information that may assist a member to deciding if they will interact. Members may also have the option to list who has viewed their profile and who is currently online.

### **Security**

This site has security measures in place to protect the loss, misuse and alteration of the information under our control. We will always do our best to protect this information and will take action against any hacking or abuse.

### **Children's Guidelines**

This site is restricted to Adults aged 18 or higher, as such any children using the site will be removed and their ISP may be notified of the abuse.

### **Choice/Opt-Out**



Our site provides users the opportunity to opt out of receiving communications from NZDating. NZDating gives users the following options for removing their information from our database to not receive future communications or to no longer receive our service. However we do also have mandatory newsletters for our members and the only unsubscribe option is to remove your membership from NZDating.

You can visit the following URL: <http://www.nzdating.com/personalise/> or visit our contact form and give us enough detail to correct the problem.

#### Correct/Update

This site gives users the following options for changing and modifying information previously provided. Visit <http://www.nzdating.com/personalise/> to personalise this web site, or visit our contact form and give us enough detail to correct the problem.

#### Contacting the Web Site

If you have any questions about this privacy statement, the practices of this site, or your dealings with this Web site, you can contact: Webmaster

NZDating

P.O.Box 44126

Lower Hutt

New Zealand

Or use our contact form

Please note: we do not provide email addresses to prevent automated spamming engines collecting them. If you need an email address please use staff at [nzdating.com](http://nzdating.com), replacing the at and spaces with the @ sign.



