ONLINE DATA PRIVACY REGULATIONS IN CHILE AND AUSTRALIA: A CRITICAL REVIEW AND FUTURE CHALLENGES

Andrés Salas Retamal*

Abstract
Privacy is still a right protected by international conventions and some domestic laws. However, it seems that data protection is not efficient in the Internet. Personal data presently has an increasing economic value, due to the spreading new and affordable technology and profuse use of social media, the amount of personal information available and generated is significantly growing each moment. Nonetheless, this easy-access technology provides several challenges for the Law to preserve data protection. In the Internet, it is difficult to enforce a practical legal framework, especially to enforce the law and cross-border flow of personal information. The discussion will be focused on a description of data protection regimes in Australia and Chile, both legal frameworks, and a critical review, particularly in the online environment. Then we will provide an overview of the international approach for cross-border personal data flow, the efforts for harmonisation and addressing the necessity of data protection authorities with appropriate faculties. Lastly, we will conclude that both Australian and Chilean systems are not entirely efficient in the Internet environment, and address some proposals to improve these legal regimes.

Key words: *Personal information, data protection, privacy, data privacy, data processing, Internet.*

1. INTRODUCTION

Privacy is a right protected by several international conventions or treaties. In several international instruments, privacy is acknowledged as a statute law given right or a constitutional right.[1] Personal data is part of this right, as being information that "identifies an individual".[2]

* (asalasretamal@gmail.com). Article received on May 19, 2018 and accepted for publication on July 26, 2018.

1 See *Universal Declaration of Human Rights*, GA Res 217ª (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/180 (10 December 1948) Art 12; *International Covenant on Economic, Social and Cultural Rights*, opened for signature 16 December 1966, 993 UNTS 3 (entered into force 3 January 1976) Art 17; *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).

2 Jackson and Hughes (2015), p. 6.

Given that personal data in Internet has high economic value,[3] its protection is increasingly challenging. The massive and constant use of social media daily contributes a colossal amount of information,[4] and actions in the Internet are not necessarily private and anonymous,[5] and the gigantic amount of personal data processed online is a complex scenario for proper data protection.[6] Consequently, not everyone is confident about the security of their information on the Internet. In Australia, only 40% of online users are "confident that privacy settings on websites work".[7] In the US, Internet users are more concerned about *web surveillance*: 86% of web users have taken different measures to "remove or mask their digital footprints".[8]

Further, while Australia and Chile have different legal and judicial regimes, they both share the need to adjust their legal data protection framework.[9] For the purposes of this work, its structure is the following: in the first section, a brief description of personal data, and its digital value will be provided. The following section presents an overview of the data privacy regimes both in Australia and Chile, and how their legal frameworks interact with the Internet. For both regimes, the discussion will be narrowed to general personal data instead of special kinds of personal information.[10] Two criteria for comparison will be used: five general data protection principles as a common standpoint for both regimes, and the challenge of law enforcement in the event of data privacy breach, particularly on the Internet environment, concluding that both regimes are weak with regards to data privacy. The next section seeks to address such failure points based on three key issues: the international approaches for cross-border data flow and the consequent need for harmonisation; and the necessity of an authority with appropriate faculties to enforce regulations. Finally, we will have concluded that both jurisdictions have insufficient data protection. However, a global harmonized approach in data privacy and a proper domestic legislation adjustment to the international standard will sufficiently improve the right to privacy with regards to personal data.

3 Jackson and Hughes (2015), p. 197.

4 In 2015, 72% of the adults in USA used Facebook, 28% Instagram, 25% LinkedIn, and 23% Twitter. While users are constantly updating "status", retweeting text and uploading pictures to Instagram, a report of June 2015 informed that Facebook ad 1,49 billion monthly active users in the world. Sloan and Quan-Haase (2017), p. 4.

5 Jay and Hamilton (2003), p. 645.

6 "The growing amount of data stored and used by firms can bring many benefits to consumers […] However, it also creates the risk of a data breach exposing large amounts of sensitive customer information". Financial System Inquiry (2014), pp. 4-55.

7 Australian Communications and Media Authority (2013), p. 1.

8 Pew Research Center (2013), p. 1.

9 The international community has addressed the need of adjustment of Australia and Chile's data protection regime, as detailed and explained in section 3 of this work.

10 Both jurisdictions have special rules for specific type of personal data, such as sensitive, financial, among others. For the purposes of this paper, we will focus only in the general personal information, and provide only a few examples of special sort of personal data.

2. PERSONAL INFORMATION AND ITS DIGITAL VALUE

Personal information (or personal data) is the information that "identifies an individual".[11] Data protection (or data privacy) is the protection of individuals against any possible unauthorised or misuse of their personal information by third parties.[12] The use of personal data is called data processing.

On the Internet, users leave and generate colossal volumes of personal data. This information is a mixture between the personal data provided by individuals themselves,[13] information provided by third parties,[14] or the information generated by the users' web surfing, called digital footprints. Digital footprint is the trace, trail or "footprints that people leave behind online".[15]

Digital footprint is the main content of "big data", which includes stores with high volumes of data, and high speed on the amount of input and output data from these banks, from a wide variety of types and sources of information.[16] This immense amount of data depends on small data inputs, such as information about people, places, sensors, cell phones, click patterns, among others. The data is generated by the everyday activities, online activities, spending habits, and communications of a given individual.[17] The idea of big data is to collect enough information about the behaviour of an individual and, with the right analytical tool, find connections and correlations among this information.[18] The result of this technique is to create accurate predictions about the future without (necessarily) the knowledge of the individual.

Personal data has high economic value. The information delivered by the Internet users to the websites (voluntarily or unbeknown), and the personal data generated (like big data) is the contemporary "new oil".[19] Personal data is the key component of our digital economy.[20] Access to (most of) web pages is free for the Internet user, and corporations make profit through advertisement. Personal information is crucial to direct such advertisement accordingly to people's interests based upon their

11 Jackson and Hughes (2015), p. 6.

12 Davara (2015).

13 For example, when filling up online forms to purchase, contract a service, navigate on a given website, or completing surveys.

14 Such as financial entities or big companies.

15 Australian Communications and Media Authority (2013), p. 14.

16 Jackson and Hughes (2015), p. 198.

17 Jackson and Hughes (2015), p. 199.

18 Lerman (2013), p. 57.

19 The term "data is the new oil" has been used since 2006 in different occasions by several individuals. It appears that the first statement with these terms was made by Clive Humby, mathematician from United Kingdom. He used the term in the Senior Marketer's Summit of the Association of National Advertisers, in Kellog School, in 2006. Palmer (2006).
The Australian Communication and Media Authority attributes this term to the World Economic Forum. *Australian Communications and Media Authority* (2013), p. 1.

20 Jackson and Hughes (2015), p. 197.

clicks. More than 90% of Google's revenues are based on advertisement.[21] In the US, more than US$2 billion are paid per year to obtain personal information from third parties.[22] Targeted ads are more effective than generic or untargeted advertisement. For instance, demographic targeting, which involves significant data collection and analysis, including "gender, location, age, race, religion, profession or income".[23] Behavioural targeting matches the users' navigation history with advertisement.[24]

3. LEGAL FRAMEWORK OF DATA PROTECTION: OVERVIEW, PRINCIPLES AND PRACTICAL CONSEQUENCES

Australia and Chile are different in their data protection legal approach. While they both have different legal systems, the international community has addressed the need of Australia[25] and Chile[26] of adjusting and improving their data protection legal standard, providing a sound opportunity of exploring the strengths and weaknesses of both jurisdictions through five common principles.[27] The analysis of the practical consequences of data privacy law breach will prove the insufficiency of data protection in both legal regimes.

21 *Alphabet Inc* (2016).

22 Zax (2011).

23 Goldberg and Wine (2012), p. 31.

24 Goldberg and Wine (2012), p. 31.

25 Several years ago, the Data Protection Working Party of the European Community issued a recommendation, addressing several concerns related to data transfer to Australia. The recommendation addressed the Australian Privacy Amendment (Private Sector) Act 2000, which contains amendments to the Privacy Act. These concerns were mainly focused on the sectors and activities excluded from the application of the Privacy Act, transparency towards data users, and use and collection for direct marketing. The opinion recommended to pursuit the improvement of the general application of the Privacy Act, for example, towards voluntary codes of conduct enforced by the Privacy Commissioner himself, or by any independent adjudicator. Article 29 Data Protection Working Party, "Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000" (Recommendation, Article 29 Data Protection Working Party of the European Community, January 2001).

26 The Chilean legal data protection system does not comply with the standard set forth by the Organisation for Economic Co-operation and Development – OECD. A Bill of Law was discussed in the Congress, with the specific purpose of adjusting the local law to the OECD data protection standard. However, this Bill was never enacted. *Boletín N° 8143-03 modifica a la ley N° 19.628 sobre protección de la vida privada* [Bill No 8143-03 which modifies Ley N° 19.628 Protection of Private Life] (Chile) 11 January 2012.

27 While both jurisdictions have different applicable principles to their data protection legal framework (and several of them are similar), for the purposes of this work we will take five common principles. These principles are -more or less- in line with the guidelines on the protection of privacy set forth by the OECD.

3.1 Australian and Chilean Data Privacy Protection Systems: an Overview

A brief overview of both Australian and Chilean data privacy protection system, including the significant similarities and differences between them will be discussed in this section. Given that Australia has a federal government, we will focus only on the federal legislation.[28]

3.1.1 Australian Data Privacy Protection System

Australian privacy and data protection are regulated in the *Privacy Act 1998* (Cth) ("Privacy Act").[29] The Privacy Act regulates the processing of personal data regarding individuals by public entities or agencies, and sensitive data (health information) processed by both public and private data controllers. "Personal information" is deemed as the information or opinion about an identified individual or a reasonably identifiable individual.[30] Thus, any given information might not be deemed as personal information on its own, but if combined with other information is identifiable or reasonable identifiable with an individual, it becomes personal data.[31] Given this broad approach, personal data might include an individual's name, address, credit information, medical records, workplace, and his or her opinions.[32]

Under the Privacy Act, individuals are entitled to protection of their personal information. As a general rule, individuals have the right to know that their personal information is being collected, how such information will be used and by whom.[33] Schedule 1 of the Privacy Act provides the Australian Privacy Principles ("APPs").[34] There are thirteen APPs and, in general terms, they refer to five basic concepts: management, collection, use and disclosure, security, and access and correction of personal information.

The first concept is reflected in APP 1 "open and transparent management of personal information"[35] and APP 2 "anonymity and pseudonymity".[36] Collection is in APP 3 "collection of solicited personal information",[37] APP 4 "dealing with unso-

28 As a federalist parliamentary constitutional state, Australia combines a "general" government (federal law) with regional governments (states). Thus, all the Australian states and territories could (and have) different legislation regarding data protection. The Privacy Act of 1998 is federal; hence, it is applicable to the entire country. To avoid different conclusions in this work, we will be focusing only in the federal law.

29 There are several state laws regarding privacy issues. However, for the purposes of this research I will focus only on the federal legislation.

30 *Privacy Act* (1998), (Cth) s 6.

31 *Office of the Australian Information Commissioner* (2015), p. 5.

32 *Office of the Australian Information Commissioner* (2015), p. 5.

33 *Office of the Australian Information Commissioner, rights and responsibilities* (2015).

34 *Privacy Act* (1998), sch 1.

35 *Privacy Act (*1998*)*, sch 1 cl 1.

36 *Privacy Act* (1998), sch 1 cl 2.

37 *Privacy Act* (1998), sch 1 cl 3.

licited personal information",[38] and APP 5 "notification of the collection of personal information".[39] Use and disclosure of personal data is reflected in APP 6 "use or disclosure of personal information",[40] APP 7 "direct marketing",[41] APP 8 "cross-border disclosure of personal information",[42] and APP 9 "adoption, use or disclosure of government related identifiers".[43] Security of personal data is in APP 10 "quality of personal information"[44] and APP 11 "security of personal information".[45] Lastly, access and correction of personal data is reflected in APP 12 "access to personal information"[46] and APP 13 "correction of personal information".[47]

Regarding security of personal information, APP 11 provides that data controllers "must take such steps as reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure".[48] However, the legislation does not convey what would be reasonable[49] to keep the information secure, and "reasonable steps" should be analysed in a case-by-case basis.[50] The Australian Information Commissioner is the authority entitled to investigate privacy complaints from individuals.[51]The Commissioner can promote conciliation between the parties, make determinations and commence proceedings; but it does not have the faculty to enforce the law by itself, even though it is entitled to file actions in order to enforce his determinations.[52] The court will analyze each case and determine if there was a law breach, and if there is merit for civil penalties.[53]

38 *Privacy Act* (1998), sch 1 cl 4.

39 *Privacy Act* (1998), sch 1 cl 5.

40 *Privacy Act* (1998), sch 1 cl 6.

41 *Privacy Act* (1998), sch 1 cl 7.

42 *Privacy Act* (1998), sch 1 cl 8.

43 *Privacy Act* (1998), sch 1 cl 9.

44 *Privacy Act* (1998), sch 1 cl 10.

45 *Privacy Act* (1998), sch 1 cl 11.

46 *Privacy Act* (1998), sch 1 cl 12.

47 *Privacy Act* (1998), sch 1 cl 13.

48 *Privacy Act* (1998), sch 1 cl 11.1.

49 According to the Office of the Australian Information Commissioner, "reasonable" and "reasonably" should be considered in "their ordinary meaning, as being bases upon or according to reason and capable of sound explanation". *Office of the Australian Information Commissioner, guidelines* (2015), chapter B 22.

50 The reasonable steps test is an objective test, and 'is to be applied in the same manner as "reasonable"'. *Office of the Australian Information Commissioner, guidelines* (2015), chapter B 23.

51 The Office of the Australian Information Commissioner will receive complaints after the individual had complained directly to the agency or organisation involved in the data security breach. If such agency or organisation does not response within 30 days, or the answer is unsatisfactory, then the individual is entitled to file a complaint at the Office of the Australian Information Commissioner.

52 *Privacy Act* (1998), pt V.

53 *Privacy Act* (1998), pt V.

In January 2015, the Office of the Australian Information Commissioner ("OAIC"), released a consultation guide on information security.[54] Although this guide is not legally binding, it was made to help government agencies and private organisations to comply with their obligations under the Privacy Act. OAIC conveys that the guide might be relevant even for organisations that are not under the scope of the Privacy Act. OAIC will refer to the guide when investigating a security information complaint.[55] In March 2015, OAIC also published guidelines to APPs,[56] to "promote and understanding and acceptance"[57] of the APPs.[58]

Regarding the consent of the data subject, as a general rule, the Privacy Act requires that consent should be express or implied,[59] while processing sensitive data[60] requires express consent.[61] The Privacy Act applies to activities engaged in Australia. It will also apply for overseas activities if there is a link with the Australian jurisdiction.[62] All of the APPs apply, in principle, to private entities and public or federal agencies or bodies. Exemptions of the Privacy Act application are media organisations (in the course of journalism), registered political parties, authorities, individual acting outside the business capacity, employer acting with regards to employee records, and small business operators.[63]

3.1.2 Chilean Data Privacy Protection System

Since June of 2018, data protection is a constitutional right in Chile.[64] Data privacy regulations are provided by *Ley N° 19.628 sobre Protección de la Vida Privada* [Protection of Private Life] ('DPA').[65]

54 According to the functions of the Commissioner provided in the Privacy Act. *Privacy Act* (1998), s 28(1).

55 *Office of the Australian Information Commissioner, guide* (2015), p. 2.

56 *Office of the Australian Information Commissioner, guidelines* (2015).

57 *Privacy act* (1998), s 28(1)(c)(i).

58 *Office of the Australian Information Commissioner, guidelines* (2015), i.

59 *Privacy Act* (1998), s 6(1).

60 "Sensitive Information" means, under the *Privacy Act*, information or opinion about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, criminal records, health information, genetic information or biometric information. *Privacy Act* (1998), s 6(1).

61 *Privacy Act* (1998), sch 1 cl 3.3.

62 *Privacy Act* (1998), ss 5B, 13D, 16C.

63 *Privacy Act* (1998), ss 7B-7C.

64 The Constitutional amendment was introduced in order to achieve a higher data protection standard in accordance with the international OECD standard, and in pursuit of the European tendency. Further, in the rest of Latin America, several countries already had this constitutional level of data protection. *Ley N° 21.096* (2018).

65 *Ley N° 19.628* (1999) DPA.

DPA provides a broad definition of personal data, as "data related to any type of information concerning identified or identifiable individuals".[66] Hence, personal data is the information of an individual in the Internet, and the information generated by the user online. The data subject can only be an individual ("natural person"),[67] not moral or legal entities.

Data bank (or data base) is any source of personal data.[68] DPA applies to the data responsible (or data collector), who could be a natural or moral person, a private entity or a government public body or agency.[69] DPA also applies to data processing, which consists in any operation or technical procedures that allow the collection, storage, recording, organization, creation, selection, extraction, confrontation, interconnection, dissociation, communication, assignment, transference, transmission or cancelation of personal data, or its use in any other manner.[70]

Given the above, the generated or provided information in the Internet will be deemed as personal data if such information can be associated to a specific individual. The data responsible will be any person that performs data processing. Considering the broad scope of data processing of the DPA, even the storage of personal data on a website[71] could be deemed as data processing.

Data processing, as a general rule, can only be performed with the prior, informed and written consent of the data subject. According to Article 4, data subjects must be informed about the sources of the data collected; the purpose for which the data is being collected; the identity of all entities or individuals who will receive the data on a regular basis; and in relation to data for surveys, market studies or public opinion polls, whether the answers are mandatory or optional.[72]

Exemptions of individual's consent are the data processing that involves freedom of speech and press activities,[73] functions or acts of authorities, national security or national practice, and information collected from public sources.[74]

DPA does not expressly set forth the principles of data privacy, but it provides the rights of the data subject and the obligations of the data controller. Individuals have the right to request information to the data user about the data it holds in connection to the data subject, its source and recipients, the purpose of the collection and storage of such data and information of the persons or entities to which his/her data is regularly

66 DPA Art 2 f).

67 DPA Art 2 ñ).

68 Data bank is, under the DPA, the "organized assembly of personal data, whether automated or not, and regardless of its form or mode of creation or organization, that allows making relations between data or any other type of data processing". DPA Art 2 m).

69 DPA Art 2 n).

70 DPA Art 2 o).

71 Such as personal data delivered or created in social media platforms, online games, among others.

72 DPA Art 4.

73 *Ley N° 19.733* (2001).

74 DPA Art 4, 9, 15, 20.

transferred.[75] Data subject also has the right to the modification of the data, in case it is wrong, imprecise, misleading or incomplete,[76] and the right to the elimination of the data, when its storage does not have a legal basis or if it has expired.[77] This right also applies when the individual wilfully authorized the use of his personal data for commercial purposes, but wishes to no longer receive such type of communication.[78]

DPA regulates transmission of personal data like data processing. Hence, communication of personal data to third parties requires the written authorisation of the data subject. "Data communication" or "transmission" is defined as "the disclosure, in any manner, of data of a personal nature to persons other than to the individual to whom such data refers, regardless of whether such persons are of determined or undetermined identities".[79] DPA does not regulate the cross-border transfer of personal data, and there are no restrictions for the transference of personal data to certain countries or jurisdictions. DPA shall apply to all the personal data collected in Chile and in relation with a data subject who is located in Chile. Thus, even though the data has been transferred abroad, the treatment of such data must be performed, in principle, according to the provisions of the DPA.[80]

Sanctions depend on the regulation breached. The data subject is entitled to exercise the rights for information, modification, cancelation or blockage of personal data by through a direct request addressed to the data controller. The data controller is required to respond within two business days. If it takes him or her more time to respond, or denies the request for any reason different than national security or public interest,[81] fines will be imposed to the data controller. Hence, the data responsible is held to strict liability. All imposed fines are for fiscal benefit, notwithstanding the data subject's general right for damages against the data controller.

There is no data protection agency or authority in Chile.[82] To enforce DPA provisions, to apply fines and to seek damages, the data subject needs to file actions before a court of justice.

75 DPA Art 12.

76 DPA Art 6.

77 DPA Arts 9, 12.

78 DPA Art 12.

79 DPA Art 2 c).

80 This application of Chilean regulations abroad is theoretical, considering the high time-consuming and costs of the procedures to enforce the Data Protection Act abroad, and that there are no specific international treaties for this regard. To our best knowledge, and up to this date, there is no case law related to the enforcement of Chilean data protection regulations offshore.

81 If the data subject challenges the argument of "national security" or "public interest" given by the data controller, it is left for the courts to decide. DPA Art 16.

82 The Council for Transparency was established by Ley N° 20.285 Transparency an Access to Public Information Act. The Council is the public body which main task is oversight the State transparency, the right to access to public information, and the procedures to exercise such right and its protection. In this sense, the Council is entitled to enforce the transparency provisions when public agencies are involved. However, a Bill of law which seeks to significantly modify the Data Protection Act is addressing the Council as the authority in charge of the oversight and enforcement of the Data Protection Act. We detail this proposal in section 4.2 of this work.

3.1.3 Analysis

Both jurisdictions have similarities and differences in the legal framework of data privacy. Given the broad definition of personal information, online provided or generated information is deemed as personal data in both regimes. DPA offers a strict liability sanction regime only regarding fines, not for damages. In Australia the data subject needs to prove damages before courts of justice, and regulations apply only to government agencies or public bodies as data controllers (except for sensitive data processing). Australia has express provisions of APPs in its legislation, a data privacy authority, and implied consent is permitted, even with the individual's silence. In Chile there is no data protection authority, express consent is the general rule, and individuals, private entities and public bodies could be deemed as data controllers.

Despite these two rather different legal approaches, both legal frameworks are insufficient for proper data protection due to their inability to abide by certain basic data protection principles. The following sections evidence these weaknesses throughout two analyses: five common data privacy principles and the practical consequences for data protection breach.

3.2 Data Privacy Principles

Data protection aims to guarantee the individuals' privacy, assuming a practical and realistic control of the use and purposes of their personal data, as well as the individual's ability to challenge this use for purposes outside the scope of his or her consent.[83] The following five principles are cross-cutting, i.e. they are the basis of most domestic laws that protects individuals' identity and information.[84]

The first principle is consent, which generally means that the data subject is the only one entitled to provide authorisation for the data processing. Exceptions include data collected from public sources and public safety. The second principle is data quality: the data which will be processed must be pertinent, adequate and delimited to the purposes of the data processing. This principle is related to the permanent bring up-to-date of the data. The third principle is the information in the data collection: the data controller must provide accurate information to the data subject, regarding the type of information collected, the purpose of the data processing, and the recipients of the information. Data controller must also inform the data subject about his or her right to access, rectification and cancellation of the information provided. The fourth principle is the transfer of personal data: the guarantee that the collected personal information will only be transferred to third parties prior consent of the data subject, and in relation to the purposes of the data processing. Lastly, the fifth is the non-discrimination principle: data processing cannot create arbitrary discrimination, with regards to race, colour, sexual life, religion, political standpoint or any other believe or conviction.[85]

83 Aponte (2007), p. 112.

84 Barrera (2013), p. 13.

85 Barrera (2013), p. 14, citing Aponte (2007), pp. 115-116.

The following analysis of the extent of the implementation of these principles in Australia and Chile is relevant to understand why both regimes are neither sufficient nor efficient to a proper data protection level.

3.2.1 Consent

(a) Australia

Section 6 of the Privacy Act provides that consent of the data subject is defined as "express consent or implied consent",[86] with no further guidance. The OAIC, in its APPs guidelines,[87] conveys that a data controller should not assume an individual's consent on the basis that the data subject "did not object to a proposal to handle personal information in a particular way",[88] even when the data processing of disclosure of the personal data "appears to be advantageous to that person".[89]

Implied consent should be taken when it can be reasonably inferred. According to the OAIC guidelines silence is "very difficult" to be taken as implied consent.[90] Therefore, consent should be voluntary and informed.[91] Consent appears to be relevant in the application of several APPs. However, it is not expressly provided as a principle. In some situations, consent "is an exception to a general prohibition",[92] like in APP 3.3(a) and APP 6.1(a). An Internet user will provide and generate different and significant personal information. Thus, consent on the processing of personal data may be easily regarded as implied, e.g. only for using or navigating in a web site, as in most of the Internet based commercial transactions. However, sacrifice of data privacy is the correct approach. With the express consent as the general rule, the data subject would have to (at least) read and acknowledge the general information of the data processed.[93]

In some circumstances, it will not be possible for the data subject to withdraw his or her consent.[94] Considering implied consent, it is (at least) questionable that an individual's silence could constitute consent. Silence should never be deemed as consent. This would have consequences such as slower business transactions. However, internet commercial transactions should not imply an unprotected data privacy system.

86 *Privacy Act* (1998), s 6.

87 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 22.

88 *Office of the Australian Information Commissioner, guidelines* (2015), chapter B, 9.

89 *Office of the Australian Information Commissioner, guidelines* (2015), chapter B, 9.

90 *Office of the Australian Information Commissioner, guidelines* (2015), chapter B, 10.

91 *Office of the Australian Information Commissioner, guidelines* (2015), chapter B, 10.

92 *Office of the Australian Information Commissioner, guidelines* (2015), chapter B, 9.

93 We are not assuming that every Internet user actually reads and understand the 'terms and conditions' or the "privacy policy" of the different websites. But the aim is to provide that information to the data user, and to have a record or proof of such consent for data processing.

94 Jackson and Hughes (2015), p. 204.

(b) Chile

Data subject's consent for data processing in the Chilean legal framework must always be informed, express and written.[95] There is no implied consent, and silence is not a form of consent. This approach provides legal certainty for both data subject and data controller, regarding the information received and the scope of the data processing.

Furthermore, there cannot be contractual clauses (like a webpage's "terms and conditions") with limitations to the rights of information (access), modification, erasure, and blocking of personal data.[96] Express consent allows the data user to acknowledge a legal basis regarding which information will be processed, the purposes of this collection, his or her rights, and the identity of the data bank. In the online environment this consent is usually reflected in a check-the-box mechanism ("I agree with the terms and conditions"). Thus, it is possible to have a record of such consent.

3.2.2 Quality of the data

(a) Australia

According to APP 10, the data controller must take reasonable steps to ensure that the "personal information it collects is accurate, up-to-date and complete".[97] OAIC acknowledges that "poor quality" of personal data might impact individuals' privacy.[98] Personal data will be accurate when it does not contain an error or defect. Up-to-date means information contemporary and current. Complete personal information presents a true or full picture (as opposed to partial or misleading picture). Personal data will be relevant if it has a connection to the purpose for which the data is being processed.[99]

(b) Chile

DPA provides that personal data must be deleted (eliminated) when there is no legal basis for registering and filing personal information. In addition, information which contains errors, mistakes, or is incomplete must be corrected/modified. Inaccurate personal data or information with doubtful validity (term) will be blocked.[100] Moreover, personal data must be accurate, up-to-date and "be truthful to the real situation of the data subject".[101]

95 DPA Art 4.

96 DPA Art 13.

97 *Privacy Act* (1998), sch 1 cl 10.1.

98 For instance, personal information with poor quality might mislead to: factual information (name, date of birth, address); a different opinion than the genuine opinion held by an individual; or lack of accreditation that an individual has subsequently obtained. *Office of the Australian Information Commissioner, guidelines* (2015), chapter 10, 2-5.

99 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 10, 4-6.

100 DPA Art 6.

101 DPA Art 9.

DPA grants the right of the data subject to request the modification of the personal data when the information is wrong, inaccurate, misleading or incomplete,[102] and the right to block or deletion of obsolete personal data or data for which there is no longer any legal basis for retention.[103]

However, it is hard to oversee the proper compliance of these provisions. For instance, the financial industry uses personal data to evaluate an individual's financial risk. Some companies might be using invalid data. And since there is no mandatory registration as a data bank or data collector, it is difficult to trace those companies.[104] A practical control from the data subject over the quality of the information could be achieved if the data protection authority kept a registry of data controllers.

3.2.3 Information

(a) Australia

A data controller will collect information if such personal data is obtained directly from the data subject, or from a "record or generally available publication".[105] APP 3 provides when and how a data bank can collect personal information. According to the OAIC, the data collector is entitled to request personal information directly, or reasonably related or when needed for its functions or activities.[106] In addition, collection should be lawful and by fair means, and, in principle, directly from the data subject. Notwithstanding the distinction between soliciting and collecting personal data, this APP applies to both activities.[107]

Although APP 3 provides that the data collecting must be performed by lawful means, the Privacy Act does not define what lawful means are. OAIC provide some examples of unlawful means, such as collecting via computer hacking or using telephone interception.[108]

According to APP 4, unsolicited personal data received by a data controller must be destroyed, de-identified and always be processed in accordance with the APPs.[109] Since unsolicited is not defined in the law, the OAIC express that unsolicited personal data is the information received without steps taken for collection.[110] APP 5 provides that data subjects must be notified as soon as practicable of the fact that their data is being collected. OAIC considers that the content of such notification must include the data collector identity and contact details, the circumstances of the

102 DPA Art 12.

103 DPA Art 12.

104 Moreover, in Chile, like in Australia, there is no explicit right to be forgotten or right to be deleted.

105 *Privacy Act* (1998), s 6(1).

106 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 3.3.

107 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 3.4.

108 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 3.14.

109 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 4.2.

110 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 4.3.

collection, if the collection is required or authorised by law, the purposes of the data processing, the consequences of not collecting the personal data, the usual disclosure of the kind of personal data collected, data of the privacy policy (if applicable), and if the personal data will be disclosed to other countries. [111] APP 12 conveys that, as a general rule, the data subject is entitled to have access to his or her information held by a data controller,[112] and APP 13 provides that the data controller must take reasonable steps to correct any personal data by request of the data subject. Such correction must be performed considering the purpose of the data processing, and accuracy, up-to-date, completeness, relevance and not misleading of the information.[113]

In direct relation with consent, implied consent is an obstacle to comply with the information principle. If consent is not express, it is difficult to properly inform the data subject. Notification (APP 5) is not equal to consent. The action of obtaining the express consent from a data subject by the data controller would necessarily involve the information of the sort or personal data collected, its purposes, the receipts of the data, and the data subject's rights regarding the data processing.

OAIC has determined that in the online environment, data collectors must take reasonable steps to make Internet users' aware of the purposes of the collection of their personal information, e.g. Internet user's IP address.[114]

(b) Chile

The data subject must be informed about the source of the data collected, the purposes of the data collection and the possible disclosure of his or her personal data.[115] DPA grants the data subject the right to request the data controller information regarding his or her personal data, sources of the data and its recipient, the purpose of the data processing, and the identity of all entities or individuals who will receive the data on a regular basis.[116]

In addition, the law provides that the personal data must only be processed for the purposes for which it was obtained.[117]

3.2.4 Transfer

(a) Australia

APP 6 provides that the data controller can only use or disclose personal data for the primary purpose of its collection, or a related secondary purpose.[118] This exam is closer to an objective view regarding the primary purpose. Regarding the

111 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 5.2.

112 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 12.1.

113 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 13.2.

114 *'HW' and Freelancer International Pty Limited* (2015).

115 DPA Arts 4, 6.

116 DPA Art 12.

117 Unless the data was created or collected from sources accessible to the public. DPA Art 9.

118 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 6.3.

secondary purpose, as a general rule and only for non-sensitive data, the data controller will perform a subjective analysis on establishing the "likelihood that an individual would reasonably expect his or her personal information to be used or disclosed for a secondary purpose".[119] The term "disclose" is not defined in the Privacy Act. The OAIC conveys that the act of disclosure of personal data is to make such information accessible to others outside the data controller or data bank. By performing this disclosure (or transfer), the disclosing party loses effective control on the personal data.[120]

The analysis presents a risk when taking the subjective approach for the likelihood of the data subject's expectation,[121] in particular with the permitted general situation.[122] Although OAIC expresses that this test is "objective",[123] likelihood is more of a case by case analysis, and depends directly on the motivation and will of each data subject. For this test to be properly objective, it requires its standards and permitted approach provided in the law. Not in the OAIC guidance, which is not binding.

To perform cross-border data transfer, the data controller must have reasonable belief that the foreign recipient has similar privacy obligations to the APPs, or take reasonable steps to ensure that the foreign data recipient does not breach the APPs.[124] The disclosure party is accountable for any acts of the foreign recipient that would breach the APPs.[125] According to the OAIC, the interaction between the APP 8 and s 16C of the Privacy Act creates a framework that encourages the data collector to seek a foreign recipient that will perform the data processing in accordance with the APPs. This is the main goal of the Privacy Act, which is "facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected".[126]

The fact that the data controller is liable for the possible breaches of APPs made by the foreign receipt is a sound example of real data protection. Considering the possible conflict of laws among the Australian legislation and the jurisdiction of the country's recipient, it is highly probable that the data importer will be bound to take all necessary safety measures to ensure that the foreign recipient will not breach the APPs. Of course, this is not 100% safe, but it is hard to visualize a scenario where the data controller will take such a high risk of breaching the law.

119 Jackson and Hughes (2015), p. 224.

120 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 6.5.

121 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 6.4.

122 The *Privacy Act* lists seven permitted general situations in section 16A. Moreover, it appears to be a situation to be analysed on a case by case basis. *Office of the Australian Information Commissioner, guidelines* (2015), chapter C, 1-8.

123 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 6.7.

124 *Privacy Act* (1998), sch 1 cl 8.1.

125 *Privacy Act* (1998), s 16C.

126 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 8.3.

In the Internet, OAIC has determined that the disclosure of the name of a website's user by the website itself on a blog is a breach of data privacy, given that such purpose is neither the primary purpose of the data collection nor a secondary related purpose. The data subject could not have reasonably expected for his personal data to be disclosed online.[127]

(b) Chile

DPA does not regulate cross-border transfer of personal data, and there are no restrictions for the transmission of personal data to certain countries or jurisdictions. Given the above, it is reasonable to assume that DPA provisions will apply to cross-border personal data transfer. DPA shall apply to all the personal data collected in Chile and in relation with a data subject who is located in Chile. Although personal data has been cross-border transferred, such data processing must be performed in compliance with the provisions of DPA.

However, the enforceability of the law at a domestic level is difficult. Data subjects would have to file actions on their own, without the support of a public agency or entity. Considering the high costs and time-consuming of international procedures, the already inefficient mechanism of data privacy protection is even less efficient.[128]

3.2.5 Non-discrimination

(a) Australia

Sensitive data has a higher level of protection in the Privacy Act. According to OAIC, data processing of this type of data might cause adverse consequences for the data subject, such as 'discrimination or mistreatment' based on the individual's race, ethnic origin or union membership.[129] Moreover, according to APP 3 the data collection must be performed only by lawful means.[130] An example of unlawful mean would be collecting personal data "in connection with, or for the purpose of, an act of discrimination".[131] In addition, while the APP 12 provides the right of the data subject to access his or her personal information, such right could be denied by the data controller if "giving that access would be unlawful".[132] OAIC conveys that unlawful activity might include unlawful discrimination.[133] Same logic is considered

127 *'HW' and Freelancer International Pty Limited* (2015), 49 [158].

128 As explained earlier, to file actions against a defendant located offshore, the data subject would have to commence an international notification and judicial process in Chile, in order to assert jurisdiction in the destination country. This process has elevated costs and is time-consuming. To our best knowledge, and up to this date, there are no international processes from Chilean data subjects attempting to assert jurisdiction abroad.

129 *Office of the Australian Information Commissioner, guidelines* (2015), chapter B, 28.

130 *Privacy Act* (1998), sch 1 cl 3.5.

131 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 3.14.

132 *Privacy Act* (1998), sch 1 cl 12.3(f).

133 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 12.12.

in APP 13, regarding the notification of correction of personal data between data controllers. If such notification leads to unlawful discrimination or harassment, the data controller might refrain from performing it.[134]

Another way of observing non-discrimination based on the personal data, is the option of choosing anonymity and pseudonymity when applicable.[135] The importance of this APP is that it enables the "individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others".[136]

These are sound grounds for preventing discrimination in the processing of personal data, particularly in the different scenarios of liability for unlawful means of data processing. Given that unlawful means are not defined by the law, and OAIC guidelines are not binding, there should be an express provision in the law forbidding arbitrary discrimination based on data processing.

(b) Chile

DPA provides the principle of non-discrimination in the data processing, but only related to financial personal data. The distributors of personal data and data banks must comply with non-discrimination in the data processing, among other principles.[137]

However, there is no general express provision for non-discrimination in data processing. It could be argued that the principles of financial data also apply to other types of data, or that discrimination challenges the general rules of data processing. It is the duty of the court of justice to interpret this provision.

Overall, several weaknesses regarding these principles are present in both jurisdictions, such as consent and no mandatory registry of data controllers. One particular defect is an authority with no faculties to enforce the law (or no authority whatsoever). The following section will analyse the practical consequences for data protection breach.

3.3 Practical Consequences for Data Protection Breach

In this section, consequences for data protection in each legal system will be analysed, with two hypothetical examples. The analysis will reveal a general insufficiency in the sanction regime.

Effectiveness of sanctions as consequence of a breach of law is a key issue regarding data privacy's legal framework. Accountability will not be achieved without efficient and practical sanctions. On one hand, misuse of personal information will

134 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 13.13.

135 *Privacy Act* (1998), sch 1 cl 2.1.

136 *Office of the Australian Information Commissioner, guidelines* (2015), chapter 2.3.

137 Other principles for finance personal data are legitimacy, access and opposition, information, data quality, finality, proportionality, transparency, limitation in use, and security on private data treatment. DPA Arts 17, 18, 19.

not always be deemed as a breach of law within data protection scope. Rather, there will be a breach of law insofar that misuse has caused harm on an individual. On the other hand, misuse or unauthorised data processing might be performed without causing any real harm to the data subject. The two legal frameworks analysed have different approaches towards sanctions and penalties. Which approach is most suitable for each of both scenarios? Two different examples of misuse of personal data will illustrate how the sanction regime works in each country. The Chilean legal framework seems to be more suitable and functional for the treatment of misuse of data privacy, given that, at least partially, it has a strict liability regime. The Australian approach is based on the effectively caused harm. However, neither approach ensures the application of sanctions.

The first hypothetical example is an individual using an Internet search engine. The digital footprint generated by the Internet search is used by a corporation to create target advertisement. Then, an unsolicited email is addressed to this person with advertisement related to the Internet search. The individual requests the suspension of the commercial communications, and nevertheless unsolicited emails are still being sent.

The second hypothetical example is an individual applying for a bank loan. Some companies are in the business of creating and keeping financial records of individuals (and other companies). This service is used to categorise the financial risk of an individual or company, using personal information regarding the financial status of the data subject. It is unlikely that a bank or financial entity will grant a loan to a person with records of cessation of payments, for instance. However, the individual already regularised his or her financial situation, but the data controller (holding the individual's financial record) does not have the personal information up-to-date.

In the first example, the data subject did not grant their express authorization to receive advertisement related to Internet searches.[138] The outcome of the misuse of the personal data is an email with advertisement. If the email is unwanted, the Internet user could delete it and/or mark the sender's address as spam, even request to the sender the suspension of the commercial communications (e.g. "unsubscribe"). It is difficult to see if that constitutes actual harm. There could be a scenario where sending an email or post mail based on personal data is detrimental per se. For example, in the US a case was once reported in which a retail store, through the digital footprint of a teenager (based on her shopping behaviour) sent to her family home advertisement related to baby items. The outcome was that the girl's family discover she was pregnant because of that advertisement.[139] But in the hypothetical situation, the assumption is that the email sent is harmless.

138 I will assume in this scenario that the consent must be prior, informed and by written, although there are jurisdictions where the data privacy regulations allow data controllers to convey in their terms and conditions that the data subject's consent is implied, or jurisdictions that have an *opt-in* system for direct marketing.

139 In 2014, the retail store "Target", in the US, collected several personal data from their customers. Using their personal information and past purchases, the store created an accurate profile for each customer, to send target advertisement. For the pregnancy prediction, the store referred to items that

In the second example, the harm from misuse of personal data is clearer. The data subject could have granted his or her authorisation for the data processing of financial personal data. However, such data was not up-to-date. If the individual had reasonable expectations (within the financial entity) of receiving the loan, and that loan was denied based on inaccurate and invalid data, then the harm is the loss of such legitimate expectation,[140] including the unfair categorisation as "risky" financial individual.

3.3.1 Australia

The approach in the Privacy Act is focused on a case-by-case basis. It is unlikely that the individual in the first example would challenge for damages in a court of justice.[141]

An action for damages in the second example will be more probable. It would be more likely for the plaintiff to argue that the data controller did not take reasonable steps to keep his personal data up-to-date. If the data subject files a complaint before the OAIC (assuming a data controller subject to OAIC's decisions), and the OAIC issues a determination, it will have to appear at the court of justice to enforce such determination with all the costs associated. It seems that the actual protection of personal data will not be achievable at reasonable costs, unless the data controller agrees to the OAIC mediation or settlement.

3.3.2 Chile

In the first example, it is unlikely that the individual will be able to prove concrete harm. However, in the DPA context, if the data subject requests the data controller the deletion of his or her personal data, and the data controller does not respond within two business days, fines will be imposed without referring to the possible harm created. Further, direct marketing is specifically regulated in the consumer protection regulations, with an *opt-out* system: if the individual expressly requests the suspension of commercial communication, and the supplier keeps sending them, it could be deemed as a law infringement. In both scenarios, sanctions could be the imposition of fines without discussing damages.

In the second example the harm that the data subject suffered is clear. Consequently, it is most likely that the court will rule in favour of the individual and award damages.

women tend to purchase in the first stages of pregnancy (calcium, magnesium or zinc supplements). The store sent customised advertisement to a pregnant teenager to her home. The father did not know that his daughter was pregnant until he had a conversation with the teenage girl, after receiving the advertisement. Wagstaff (2012).

140 There might be an infinite amount of reasons of why the person requested that loan. Any of them could be taken as the *harm* made by the data controller. For example, the need for a plane ticket to travel overseas and settle a huge business deal, the payment of a tuition fee on an academic institution, buying a house, among several others.

141 The Office of the Australian Information Commissioner does not have the faculty to impose fines or sanctions. It requires filing judicial actions before a court of law.

There is no data protection agency or authority in Chile. To enforce the DPA, apply fines, and seek damages, the data subject needs to file actions directly before the court of justice. In both examples, the plaintiff would have to prove the facts and harm, with all the costs associated to judicial actions. Reality has proven that there is no proper data protection through these mechanisms.

3.3.3 Analysis

Australian data privacy framework will only apply, as a general rule, to public bodies.[142] While in Australia there is an agency that receives complaints regarding data privacy, it does not seem effective for proper data privacy protection. In 2014 and 2015, the OAIC received 2,841 complaints, and closed 1,976 of them. Of the latter, 34.2% were object of an investigation, while 36.4% were closed without investigation.[143] During that period, OAIC issued seven determinations.[144]

The OAIC does not have the power to enforce the law. Data responsible might voluntarily comply with OAIC considerations. However, if there is no will from the data controller, then it will be necessary to file actions before a court of justice, with all the costs implicated.

In Chile there is no agency or authority for data privacy matters. Jurisdiction over data processing activities is limited to the Chilean courts. While Chilean courts can award damages and apply fines, the decisions of the courts, as in most civil law systems, do not produce binding jurisprudence. Rather, the courts' decisions will help to facilitate interpretation of the law in future cases.

Approximately 70 Supreme Court decisions have been issued since the enactment of the DPA in 1999 until July 2018, for breach of the law.[145] As a matter of access to justice, this small enforce of the DPA might be due to the cost of the judicial process, ineffective judicial mechanisms and poorly drafted provisions.[146] DPA is a data protection law that grants several rights but without efficient ways to enforce such rights, and without a data protection authority. In this scenario, some have characterized the DPA as a "wolf with no teeth",[147] and there is a consensus among the scholars about the

142 Unless sensitive information is subject to data processing.

143 *Office of the Australian Information Commissioner, annual report* (2015), p. 67.

144 *Office of the Australian Information Commissioner, annual report* (2015), p. 74.

145 There is an inconsistent and fairly unpredictable case law regarding the Data Protection Act. It appears to be widely mentioned in different judicial actions –among several other regulations–, but its application is finally dismissed in the final ruling. Further, a huge amount of constitutional actions is filed on the grounds of a remedy for protection of the individual's rights, mentioning and invoking Data Protection Act. However, these ruling are addressed to protect the constitutional right, hence, even when ruling in favour of the data subject, the judges cannot award damages nor impose sanctions. In any case, these rulings on remedies of protections are shifting among different decisions, without a regular line. According to www.poderjudicial.cl (last visited in July 2018), of 124 cases related with the Data Protection Act, only 74 actually apply this regulation.

146 Silva (2015).

147 Silva (2015).

key defects of Chilean data privacy regulations: lack of effective sanctions, no cross-border regulation, the *opt-out* system[148] in direct marketing which would not be an express consent,[149] wide exceptions for the data user's consent, ineffective guarding judicial procedures, and the lack of a public control agency, among others.[150]

Consequently, both legal systems, Australia and Chile, present significant differences and impediments for a proper personal data protection.

4. SOLUTIONS?

The previous section explained how domestic legal regimes are not able to provide proper data protection. In our opinion, key issues to address this matter lie on the international approaches for cross-border data flow and the consequent need for harmonisation; and the necessity of an authority with appropriate faculties to enforce regulations -(an effort of a Chilean authority to enforce data protection in the Internet before a court of justice will illustrate this necessity).

4.1 Cross-Border Data Processing and Harmonisation

Cross-border data processing could be deemed as a data processing that consists of the transmission or transportation of personal data which is carried abroad by whom is responsible for such, and transmitted directly to the natural or legal person who must receive it in a third country, so to be subject to new data processing, by himself or on behalf of the data transfer.[151]

The cross-border flow of personal data is currently increasing significantly, given the technological developments, connectivity and Internet,[152] due to data flow within the private sector and public entities. In the private sector, private multinationals need to keep information flowing among their different offices, and it is highly attractive the procurement of services in countries with low cost for data processing, e.g. call centres, technical support. Regarding public entities, agencies of different countries exchange personal data. Reasons for this exchange might be national security, international cooperation, terrorism, among several others.[153]

148 This system does not require a prior consent for the commercial communication: *opt-out* means the data subject receives the direct marketing, and after the reception, the individual has the right to request the suspension of the communications.

149 Some scholars believe that the so-called "browse agreements" (user's acceptance based on the fact of browsing a web site) have no consent at all, hence, "in all of those cases the use of [personal] data is illegal". De la Maza and Momberg (2017), p. 53.

150 Viollier (2017), p. 4.

151 Matus and Montecinos (2006).

152 European Commission (2010).

153 Guasch (2012), p. 416.

In the cross-border flow context, there will be always one data exporter (sender of the personal information) and one data importer (receiver of the personal information). One of the key issues regarding this international flow is the legal framework that protects these interexchange, and the capacity of the data receiver to legally adapt to such legal framework.[154] In other words, when the legal protection of international flow of personal data is established, the receiving party will have to comply with such legal standard.

Considering the above, a proper solution could be, for instance, harmonisation. In this regard, old Directive 95/46/CE of the European Parliament and the Council sets forth that each state must guarantee the free circulation of personal data among state members,[155] acknowledging that data privacy legislation might have different protection standards between the state members. The Directive and domestic legislations recommend performing the cross-border data flow only to state members with proper protection.[156] The Directive was repealed by the Regulation 2016/679, General Data Protection Regulation ('GDPR').[157] This regulation provides harmonization of each data protection regulation in the European Union, entailing the application of the GDPR to cross-border data transfer when performing data treatment to data subjects who are residents in the European Union, even if the data controller is located outside the Union.[158]

Another sound example of a harmonisation effort is the *Trans-Pacific Partnership Agreement* ('TPP'),[159] which involves Australia and Chile, among other countries. TPP provides that each State member must adopt a legal framework 'that provides for the protection of personal information of the users of electronic commerce',[160] and personal information is deemed 'any information, including data, about an identified or identifiable natural person'.[161] TPP expressly forces each State member to permit cross-border transfer by electronic means 'including personal information, when this activity is for the conduct of the business'.[162] Some scholars are concerned of the lack of definition of conduct of the business: because of this wide approach, it could involve all forms of business, including non-commercial purpose.[163]

154 Barrera (2013), p. 14.

155 *Directive 95/46/CE of the European Parliament and of the Council* (1995).

156 *Directive 95/46/CE of the European Parliament and of the Council* (1995), Art 25.

157 *Regulation (EU) 2016/679 of the European Parliament and of the Council* (2016).

158 *Regulation (EU) 2016/679 of the European Parliament and of the Council* (2016), p. 101.

159 *Trans-Pacific Partnership Agreement* (2016) (not yet in force).

160 *Trans-Pacific Partnership Agreement* (2016), Art 14.8.

161 *Trans-Pacific Partnership Agreement* (2016), Art 14.1.

162 *Trans-Pacific Partnership Agreement* (2016), Art 14.11.

163 Ow (2015).

Australian and Chilean legislation should follow the example of harmonisation from the GDPR. This approach would make the future provisions of the TPP applicable in the commercial relations between these two countries.

4.2 Data Protection and Internet: The Need for a Data Protection Authority

Colossal amount of personal data is processed through the Internet, delivered by the data user or created by the use or navigation in a website. Although the Internet is not a legal entity and there is no authority overseeing it, it does not mean that the Internet escapes from any sort of regulation.[164] For example, the European Court of Justice ruled in 2014 that in specific circumstances, individuals have the right to request online search engines to remove links with their personal data.[165] This is known as the right to be forgotten.[166] But the effectiveness of these sorts of regulations is doubtful, or at least establishes challenges that are not present in the real world.

Actions in the Internet are not necessarily private and anonymous.[167] Some scholars believe that the use of mobile devices that generate big data reveals sensitive data of the individual (behaviour, religious beliefs and sexual preferences, among others), but grants no control of the data subject over their personal data.[168] While the Internet transactions are increasing and becoming more complex, the privacy threats also increase with them.[169]

Due to the rapid changes of technology,[170] it is unlikely to anticipate to its changes.[171] Thus, technologically neutral regulations, which means providing principles and clear legal obligations, but not a specific or particular step-by-step on how to comply with. Perhaps that is the reason for privacy commissioners to develop guidelines for the statutory privacy law application, like the OAIC.

Due to this the lack of online security regulations for personal data, government agencies try to use consumer protection regulations or unfair competition legislation to make data controllers responsible for information security.[172] In some jurisdictions, a failure to keep information secure may be interpreted as a breach of consumer protection or trade practices obligations.[173]

164 Jay and Hamilton (2003), p. 637.

165 These circumstances are when the personal data is inaccurate, inadequate, irrelevant or excessive for the purposes of data processing. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014), 317.

166 Jackson and Hughes (2015), p. 65.

167 Jay and Hamilton (2003), p. 645.

168 DPM, *Data Privacy Management, and Security Assurance* (2016), p. 245.

169 DPM, *Data Privacy Management, and Security Assurance* (2016), p. 217.

170 Jackson and Hughes, (2015), p. 134.

171 Koltay (2014), p. 65.

172 Such as the Federal Trade Commission of the United States of America and the Financial Services Authority of the United Kingdom. Jackson and Hughes (2015), p. 140.

173 Jackson and Hughes (2015), p. 143.

In Chile, the *Servicio Nacional del Consumidor* [National Consumer Service] ('SERNAC' by its Spanish acronym) has filed several actions in pursue of the DPA compliance. These actions are always filed in the context of a breach of *Law No. 19,496 Sobre Protección de los Derechos de los Consumidores* [Law No. 19,496 Consumer Protection Act] ('CPA').[174] The authority seeks to enforce consumer's data privacy rights, when they have been breached by a supplier under the CPA. These claims are not addressing the right to *opt-out* from commercial communications (such as emails); as explained earlier, such right is not in the DPA, is granted in the CPA.[175]

SERNAC, in its law suits, has argued that CPA is applicable when the collective interest of the consumers is affected, particularly when the breach of consumers' data privacy rights arose from a consumption act. The application of the CPA in data protection cases was initially accepted by the Supreme Court,[176] given that the DPA possess an individual scope of protection; while the CPA protects the collective interest of consumers.[177] However, in the last of these claims, and in the context of a class action against the terms and conditions and the privacy policy of a supplier's Internet website,[178] the Supreme Court definitely rejected the conversation between consumer and data protection regulations.[179]. The main argument of the Supreme Court for this rejection was that the DPA is essentially individual, without collective procedures.[180]

A special concern emerged from this ruling of the Supreme Court: it appears that the application of the CPA would be logical, given that there is a consumption relationship, a standard form agreement, and the collective interest of consumers was affected.[181]

There is a solid legislative effort in adapting the current data protection legal regime. The Chilean Congress is discussing a Bill of Law which aims to amend the DPA in accordance with the OECD standards, creating a Data Protection Agency.[182] One of the last indications to this Bill sets forth that the Council for Transparency[183] will be this agency. It is not possible to anticipate if this law reform will be enacted nor when would this happen.

174 *Ley N° 19.496* (1997).

175 *Ley N° 19.496* (1997), Art 28 B.

176 *Servicio Nacional del Consumidor v Ticketmaster* (2016).

177 *Servicio Nacional del Consumidor v Créditos Organización y Finanzas S.A.* (2016).

178 A website had in its privacy policy several "abusive" clauses in terms of the Consumer Protection Act, including the limitation of the rights granted by the Data Privacy Act. Under the Consumer Protection Act, terms and conditions of use, including privacy policy, are deemed as 'standard form agreement'; according to consumer protection regulations, these kinds of agreements cannot have abusive clauses. *Ley N° 19.496* (1997), Art 16.

179 *Servicio Nacional del Consumidor v Ticketek* (2016).

180 *Servicio Nacional del Consumidor v Ticketek* (2016).

181 Momberg (2017), p. 362.

182 *Boletines 11144-07 y 11092-07 refundidos* [Merged Bills Nos. 11144-07 and 11092] (Chile) January and March 2017.

183 See above note 82.

4.3 Proposals

The following proposals are broad enough to fit in the current or in a new legislation.[184] Extensive concepts and principles make data privacy regulations work, mostly, with an ex-post basis and narrow the prevention of law breach. This sort of approach encourages several difficulties in the enforceability of the law. If a regulation is meant to be applied in the online environment, it should properly address the legal scope of its provisions.

First, data privacy in the online environment will be achieved if all Internet users grant their express consent for data processing. The data controller will be forced to inform the data subject regarding the data collected, the purposes of the data processing and the data subject's rights, as well as the identification of the data user or controller. The check-the-box mechanism is suitable for these purposes. Not every Internet user actually reads the terms and conditions,[185] but this mechanism grants legal certainty.

Second, jurisdictions should have a public agency dealing with data privacy issues, especially online matters. Although Australia has an authority in this sense, it is not empowered to enforce the law. In the Chilean case, notwithstanding the constitutional right to the protection of personal data, there is no authority whatsoever. A public agency (national bureaus or an ombudsman) in charge of data privacy matters should deal with data subject's complaints, data collectors enquiries, and have the power to impose administrative sanctions (such as fines) and to administratively interpret the law. Consequentially, authorities will not be forced

184 Extent and limits of these each proposal should be carried on with a technical support, i.e. figures and statistics of each country. Besides the Bill of Law explained in section above 4.2, to provide specific changes to the existing statutes of law or to propose new regulations are beyond the scope of this paper. Moreover, we are aware of several past and ongoing efforts in both Australian and Chilean legislation to improve data protection regulations. For example, the Chilean Congress is discussing a bill of law which provides the data subject's right to be forgotten.

For Australia, see Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Final Report No 123 (2014); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008).

For Chile, see *Boletín N° 10819-07 modifica a la ley N° 19.628, sobre protección de la vida privada, para sancionar el tratamiento irregular de datos personales* [Bill No 10819-07 which modifies Law No 19,628 Protection of Private Life, which sanctions the irregular processing of personal data] (Chile) 2 August 2016; *Boletín N° 10608-07 modifica a la ley N° 19.628, sobre protección de la vida privada, para efectos de garantizar, al titular de los datos personales, el derecho al olvido* [Bill No 10608-07 which modifies Law N° 19.628 Protection of Private Life, for purposes of guaranteeing the right to be forgotten of the data subject] (Chile) 7 April 2016.

185 In 2010, a videogame website, in its terms and conditions, expressed that every Internet user who make a purchase on 1 April 2010, would grant the website a "non transferable option to claim, for now and for ever more, your immortal soul", unless they click on a link within the terms and conditions to "nullify" this "soul transfer". Over 7,500 users did not read the terms and conditions and did not click on the link, 'transferring' their souls to the website. The Internet gaming store expressed, after one user actually clicked on the terms and conditions, that they performed the prank-experiment to prove that only "12 percent of purchasers" read terms and conditions when buying online. Smith (2010).

to use competition or consumer regulations for data protection matters. The access to this administrative procedure should be of low cost (or free) for individuals. An informal process is advisable. To observe the due process, the resolutions of these agencies could be reviewed by a court of law.

Third, these agencies should have the power to anonymise an individual by his or her request from an online environment. If there are solid grounds to believe that the identity of an individual was acquired from a data collector in breach of data privacy, the data subject will have the right to request the agency to enforce his or her anonymity.

Finally, GDPR is a great example and guidance towards harmonisation: given that the regulation is within the GDPR, there is no need for adjustment from each domestic legislation. Considering that neither Australia nor Chile are part of the European Union, TPP is a good opportunity to achieve harmonisation in data privacy regulations between Australia and Chile, e.g. all individuals and entities capable to perform data processing should be subject to data privacy regulations.[186]

5. CONCLUSIONS

Of all registered and recorded data in human history, the majority of it has been created since 2010.[187] Permanent connectivity to the web, and the endless interaction between users and websites generates an increasing amount of information and data never seen before. Personal information has an enormous commercial value. And with the massive amount of personal data online, it appears that in the Internet privacy is no longer a social norm.[188]

Overall, data privacy regulations in the Internet are not working properly. While privacy is a right legally protected, data privacy regulations are narrow in Australia, and have several challenges of enforceability in Chile. These regulations are working on an ex-post basis, without proper prevention.

Although the law should always remain technologically neutral, an extremely wide approach is not suitable for proper regulation in the online environment. To have the principles of data privacy (like the Australian law) provided in the law encourages judicial rules closer to the actual protection. However, it is against the data protection, for example, to provide "reasonable steps" with no definition. A strict liability regime is more suitable for data protection, particularly on the Internet.

Australia does have a data protection authority, but its lack of powers to enforce the law refrains it from a proper protection. In Chile, numerous court decisions are related to the DPA, but only 70 app. Supreme Court decisions are directly applying data protection regulations in the last 19 years. Laws with several rights but not proper practical approaches are, namely, the wolves with no teeth.

186 In the Australian legal framework, only public agencies are subject to the *Privacy Act*, unless sensitive information is subject to data processing.

187 Shirky (2013).

188 Johnson (2010).

Moreover, the challenges that arise in data processing are quite similar between domestic and cross-border level. Cross-border flow of personal data is increasing significantly day by day. What would constitute a proper protection? A solid legal regime on data privacy in each domestic legislation would promote in the international connection an overall efficient international legal framework. Cybersecurity will be a key challenge in the cross-border data transfer, particularly when freedom of data and information flows are adopted principles, e.g. TPP.[189] This treaty is a solid (but still risky) chance to accomplish a harmonised data protection legal regime among each of their members, and achieve proper data privacy legal frameworks. If the harmonisation among the jurisdictions is not accomplished, an adjustment of the domestic data protection legislation is urgent, in order to achieve the international standards, e.g. OECD standards.[190]

The consent for the data processing should be the key issue for Australia and Chile. In the online environment, it should be the general rule. Data subjects, with the enormous amount of personal data in the Internet, should have a proper mechanism to exercise their data privacy rights. While some individuals have their personal data successfully deleted or removed from certain data controllers in the Internet, we are still far away from a real and practical right to be forgotten. In the near future, it does not seem like the right to be forgotten in the Internet will be achievable. The question is apparently beyond that right: the extent of anonymity in the Internet. There is no simple solution, "in the absence of universally shared philosophy".[191]

189 *Trans-Pacific Partnership Agreement*, Arts 14.11, 14.13.

190 For example, Chilean scholars are deeply concerned regarding the necessity of the adjustment of the data protection legislation, in order to achieve the OECD's international standards. In this regard, "the enactment of a new law is the most remarkable opportunity […] to have a regulation focused in the protection of the individuals' rights', particularly considering that, in Chile, after 17 years of the Data Protection Act 'there is consensus among the academy and the civil society regarding the weakness in personal information regulation". Viollier (2017), p. 47.

191 Jackson and Hughes (2015), p. 73.

BIBLIOGRAPHY CITED

Alphabet Inc. (2016): "Alphabet Announces Second Quarter 2016 Results", available at: https://abc.xyz/investor/news/earnings/2016/Q2_alphabet_earnings/index.html

Article 29 Data Protection Working Party of the European Community, "Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000", Recommendation, January 2001, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp40_en.pdf

Aponte, José (2007). "La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano", *Revista de Derecho Privado*, N° 12-13, pp. 109-124.

Australian Communications and Media Authority (2013): "Digital footprints and identities – Community attitudinal research", in: http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Digital%20footprints%20and%20identities%20community%20attitudinal%20research%20pdf.pdf

Australian Communications and Media Authority (2013): "Privacy and personal data – Emerging issues in media and communications – Occasional paper 4", available at:

https://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Privacy%20and%20digital%20data%20protection%20Occasional%20paper%204.pdf

Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report N° 108 (2008).

Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Final Report N° 123 (2014).

Barrera, Isabel (2013): *Estado Situacional de la Protección de Datos Personales en Chile, Regulación Jurídica y Alcances* (tesis de maestría, Universidad de Chile, 2013), available at: http://www.repositorio.uchile.cl/handle/2250/115456Davara, Miguel Ángel (2015). *Manual de Derecho Informático* (Aranzadi).

De la Maza, Iñigo y Momberg, Rodrigo (2017). "Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web", *Revista Chilena de Derecho y Tecnología*, N° 2, Vol. 6, pp. 25-55.

European Commission (2010): "Europeans' Privacy will be big challenge in next decade, says EU Commissioner", available at: europa.eu/rapid/press-release_IP-10-63_en.htm

García-Alfaro, Joaquín *et. al.* (eds.) (2016). *Data Privacy Management, and Security Assurance: 10th International Workshop, DPM 2015 and 4th International Workshop, QASA 2015, Vienna, Austria, September 21-22, 2015: Revised Selected Papers* (Springer).

Financial System Inquiry (2014): "Interim Report", available at: fsi.gov.au/files/2014/07/FSI_Report_Final_Reduced20140715.pdf.

Goldberg, Paul W. y Guo, Mingyu (eds.) (2012). *Internet and Network Economics: 8th International Workshop, WINE 2012, Liverpool, UK, December 10 - 12, 2012 ; Proceedings* (Springer).

Guasch, Vicente (2012). "La Transferencia Internacional De Datos De Carácter Personal", *Revista de Derecho UNED,* N° 11, p. 413.

Jackson, Margaret y Hughes, Gordon L. (2015). *Private Life in a Digital World* (Pyrmont, Thomson Reuters).

Jay, Rosemary y Hamilton, Angus (2003). *Data Protection: Law and Practice* (Sweet & Maxwell).

Johnson, Bobbie (2010): *"Privacy no longer a social norm, says Facebook founder"*, available at: www.theguardian.com/technology/2010/jan/11/facebook-privacy

Koltay, András (ed.) (2014), *Media Freedom and Regulation in the New Media World* (Wolters Kluwer Ltd. CompLex Kiadó).

Lerman, Jonas (2013): "Big Data and Its Exclusions", *Stanford Law Review Online,* Vol. 66, pp. 55, available at https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_stanlrevonline_55_lerman.pdf.

Matus, Jessica y Montecinos, Alejandro (2006). *El deber de información y el consentimiento para la cesión de datos personales* (Lexis Nexis).

Momberg, Rodrigo (2017). "Acciones colectivas y ley N° 19.628 sobre protección de la vida privada y de datos de carácter personal", *Revista Chilena de Derecho Privado*, N° 28, pp. 357-363.

Office of the Australian Information Commissioner (2015): "Annual Report 2014-15", available at: www.oaic.gov.au/resources/about-us/corporate-information/annual-reports/oaic-annual-report-201415/oaic-annual-report-2014-15.pdf.

Office of the Australian Information Commissioner (2015): "Australian Privacy Principles guidelines", available at: https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf.

Office of the Australian Information Commissioner (2015): "Guide to securing personal information – 'Reasonable steps' to protect personal information", available at: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf.

Office of the Australian Information Commissioner, (unknown date): "Rights and responsibilities", available at: www.oaic.gov.au/privacy-law/rights-and-responsibilities.

Ow, Jack (2012): "The Trans-Pacific Partnership's take on personal data", available at: united-kingdom.taylorwessing.com/globaldatahub/article-the-tpp-take-on-personal-data.html.

Palmer, Michael (2006): "Data is the New Oil", available at: ana.blogs.com/maestros/2006/11/data_is_the_new.html.

Pew Research Center (2013): "Anonymity, Privacy, and Security Online", available at www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf.

Shirky, Clay (2013): "How very wrong David Simon is about the NSA's capabilities", available at: www.theguardian.com/commentisfree/2013/jun/12/david-simon-wrong-nsa-capabilities.

Silva, Paulina (2015): "The regulatory framework for data protection in Chile and Future Challenges", available at: united-kingdom.taylorwessing.com/globaldatahub/article_dp_cyber_chile.html.

Sloan, Luke y Quan-Haase, Anabel (eds.) (2017), *The SAGE Handbook of Social Media Research Methods* (SAGE reference).

Smith, Catharine (2010): "7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation", available at: http://www.huffingtonpost.com.au/entry/gamestation-grabs-souls-o_n_541549.

Viollier, Pablo (2017). *El estado de la protección de datos personales en Chile* (Derechos Digitales).

Wagstaff, Keith (2012): "How Target Knew a High School Girl Was Pregnant Before Her Parents Did", available at: techland.time.com/2012/02/17/how-target-knew-a-high-school-girl-was-pregnant-before-her-parents.

Zax, David (2011): "Is Personal Data the New Currency?" available at: www.technologyreview.com/s/426235/is-personal-data-the-new-currency

LEGISLATION CITED

Australia:

Privacy Act (1998) (Cth).

Chile:

Ley N° 19.628 sobre Protección de la Vida Privada [Law N° 19.628 Protection of Private Life], August 28th, 1999.

Ley N° 19.733 sobre las libertades de opinion e información y ejercicio del periodismo [Law N° 19.733 of Freedom of Speech and Journalistic Activities], June 4th, 2001.

Boletín N° 8143-03 modifica a la ley N° 19.628 sobre protección de la vida privada [Bill N° 8143-03 which modifies Law N° 19.628 Protection of Private Life], 11 January 2012.

Boletín N° 10608-07 modifica a la ley N° 19.628, sobre protección de la vida privada, para efectos de garantizar, al titular de los datos personales, el derecho al olvido [Bill No 10608-07 which modifies Law N° 19.628 Protection of Private Life, for purposes of guaranteeing the right to be forgotten of the data subject], 7 April 2016.

Boletín N° 10819-07 modifica a la ley N° 19.628, sobre protección de la vida privada, para sancionar el tratamiento irregular de datos personales [Bill No 10819-07 which modifies Law N° 19.628 Protection of Private Life, which sanctions the irregular processing of personal data], 2 August 2016.

Ley N° 21.096 consagra el derecho a protección de los datos personales [Law N° 21.096 enshrines the right to the protection of personal data], June 16th, 2018.

European Union:

Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature November 4th, 1950, entered into force on September 3rd, 1953.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

International Treatises:

International Covenant on Economic, Social and Cultural Rights, opened for signature December 16th, 1966, entered into force January 3rd, 1976.

Trans-Pacific Partnership Agreement, signed February 4th, 2015, not yet in force.

United Nations:

Universal Declaration of Human Rights, December 10th, 1948.

CASES CITED

Australia:

'HW' and Freelancer International Pty Limited, AICmr 86 (2015). Office of the Australian Information Commissioner, December 18th, 2015.

Chile:

Servicio Nacional del Consumidor v Créditos Organización y Finanzas S.A. (2015). Supreme Court, October 11th, 2016, Case No. 4903-2015 (abusive clauses in standard form agreements between suppliers and consumers).

Servicio Nacional del Consumidor v Ticketmaster (2015). Supreme Court, July 7th, 2016, Case No. 1533-2015 (abusive clauses in standard form agreements between suppliers and consumers).

Servicio Nacional del Consumidor v Ticketek (2015). Supreme Court, December 6th, 2016, Case No. 26932-2015 (abusive clauses in standard form agreements between suppliers and consumers).

European Union:

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014). European Court of Justice, May 13, 2014, Case No. C-131/12, *ECLI identifier: ECLI:EU:C:2014:317.*