The Problem to Consent to the Collection, Use, and Disclosure of Personal Information in Cyberspace

Thilla Rajaretnam
Associate Lecturer, School of Law,
University of Western Sydney, NSW Australia
E-mail: t.rajaretnam@uws.edu.au

Abstract - Consumer concerns over the safety of their personal information and the violation of their privacy rights are described as being the single overwhelming barrier to rapid growth of e-commerce. This paper explores the problems for e-commerce users when there is collection, use, and disclosure of personal information that are based on implied consent in e-commerce transactions. It questions the assumption that consent is sufficient to waive privacy interests in relation to e-commerce transactions. It will argue that consent should not necessarily be sufficient to waive privacy interests, and that the collection, use and/or disclosure of personal information should be subject to regulation.

Keywords: *Privacy, consent, e-commerce, risks to personal information, regulation*

I. INTRODUCTION

Information technology has affected privacy dramatically [1] [2]. The internet has made it possible for any person to easily collect personal information about Internet users and others including e-commerce users with or without their consent. Consumer concerns over the safety of their personal information and the violation of their privacy rights are described as being the single overwhelming barrier to rapid growth of e-commerce. Recent research findings also show that the level of public concern for privacy and personal information has increased since 2006 [1] [3]. In 2007, it was found that 50 percent of Australians are more concerned about providing information about them online than they were two years ago [4].

This paper explores the on constraints on the exercise of individual autonomy. Viewed from the perspective of autonomy, it considers what autonomy means for these purposes and whether current practices (such as the use of standard-form privacy policy statements, bundled consent) protect individual autonomy. It argues that to resolve the problem with allowing the use and/or disclosure of personal information based on consent, the e-commerce user must first have sufficient knowledge of the purpose for information collection, its use and disclosure of information collected; secondly, consent mechanisms should allow informed and rational decision making; thirdly, there should be the opportunity for individual choice allowing withdrawal of consent or the opting out of information collection. It questions the assumption in most legislation which affects e-commerce users, that consent is sufficient to waive an individual's privacy interests..

This paper will discuss firstly, the issue of privacy in the e-commerce context of information privacy; secondly, examine the meaning and role of consent in relation to the collection, use and disclosure of personal information in cyberspace; thirdly, if individuals have freedom of choice; fourthly the threats to privacy interests and the problems that arise for individuals when there is collection, use and disclosure without consent; and finally, this paper briefly examines what information privacy protection there is under the current framework international, regional and national framework in Australia. In the process it will explore some possible solutions to the problem of online privacy for individuals.

II. PRIVACY

A threat to privacy will be a threat to the integrity of a person [5] and it is the right of each individual to protect his or her integrity and reputation by exercising control over information about them which reflects and affects their personality [7] [8]. The important elements of the right to privacy are identified by theorists, [5] [6] [7] as being "the right to be left alone" [5]; and to be anonymous as one of the important elements of privacy. The right of an individual to control such information enables that individual to selectively restrict others from his or her physical and mental state, communication and information, and control how the person wishes to be presented, to whom and in which context [7] [8].

Control over information is connected to how individuals want to be seen, to whom they want to be seen, and in what context [6] [7]. The disclosure facts that are considered personal and intimate will expose and reveals an individual's vulnerability and psychological processes that are necessarily part of what it is to be human [7] [8]. This capacity to control disclosure is seen an element of personal integrity, reputation, human dignity, expectations, autonomy and self determination, happiness and freedom [7] [8] [9]. The individual's ability to control disclosure of facts about themselves is valued as a means of protecting personality rather than property interests [7]. Control includes the ability to consent, make decisions and choices whether to allow or disallow others into the individual's private space and information about them.

III. CONSENT

Consent is an expression of individual autonomy, and the right for individuals to make decisions about how they will live their lives. In the context of information privacy, consent is the mechanism by which the individual e-commerce user exercises control over the collection, use or disclosure of personal information. Consent to the disclosure of private information provides the basis for an e-commerce user's agreement to the collection, use, access and transfer of personal information.

Most often e-commerce users may have expressly agree to the collection, disclosure and use of information beyond what is required for the immediate transaction [10] [11]. Express consent may be given in a variety of ways by e-commerce users such as when filling in a form online, or by ticking on a tick box provided on a website. Consent might be also implied from the previous conduct of the parties or through an existing business or other relationship where it can be assumed that an individual has reasonable expectation of receiving information; or where the individual has reasonable expectation that their personal information may or will be collected [12] [13].

According to normal legal principles, consent cannot be effective if the person does not have sufficient knowledge or understanding to consent. Before e-commerce users can make a considered decision whether to consent, they must have some understanding of the implications of what is being consented to, and sufficient detail in language suitable for e-commerce users to give genuine consent [13]. There is the added problem relating to young persons and others who may lack legal capacity to consent. Tied to consent is the exercise of choice by the individual.

IV. CHOICE

A secondary sense in which autonomy is used is that it requires freedom of choice [10] [11]. Control over personal information enables an autonomous individual to make choices, and to select those persons who will have access to their body, home, decisions, communication, and information and those who will not. In e-commerce, individuals make choices about the use and disclosure or surrender of their personal information for secondary purposes. The e-commerce user's ability to exercise autonomy as deliberative choice is constrained in a number of ways. Firstly, choice requires the individual to be a rational consumer making informed and considered decisions and having options in relation to their personal information. The options that are available to individuals in cyberspace to collection, use and the sharing their personal information is the opt-in and opt-out regime. There are also different views on the efficacy of opt-in versus the opt-out regime. On one view this could be considered consent by trickery while the other view is that there is no true choice [11]. For example, if individuals do not actively select to opt out then they are taken to agree by default. The box may also be ticked as the default state to indicate agreement with the consumer required to 'untick' the box if they do not agree. The e-commerce user is unlikely to fully appreciate the effect and importance for their privacy of ticking a box agreeing to the terms and conditions of access to the website or the transaction. Secondly, there are significant barriers to the effective exercise of autonomy when e-commerce users have difficulty in locating the provider's privacy policy. Available evidence suggests that only a very few e-commerce users exercise autonomy in this sense; users seldom read privacy clauses on websites or change their behaviour as a consequence [15] [16]. Information may not be easily accessible, or difficult to find, or in legal language which is not easily comprehended, or may be lengthy and vague as to exactly what is being agreed or what rights they are actually surrendering [16] [11].

Thirdly, an e-commerce users' choices whether to access a website may be constrained if required to agree to terms and conditions up front or may find that alternatives are equally constrained. Similarly if other providers have similar policies which do not allow the user to refuse the terms and conditions, the e-commerce user will lack autonomy in this secondary sense.

Fourthly, an e-commerce user' ability to exercise autonomy is further compromised by the use of bundled or blanket consent used by data collectors and e-business operators [11]. Bundled consent refers to the consent to a wide range of uses and disclosures without giving an individual the opportunity to make a choice about which use or disclosure they agree to and which they do not. Bundled consent frequently includes terms and conditions allowing changes to privacy policies without notice. The use of bundled consent cannot be meaningful because the person who consents to such terms and conditions does not know what he or she is consenting to. One reason being that privacy clauses containing bundled consent are usually lengthy, often in very small font size and may not be easily accessible [12] [16]. Data collectors are also using bundled privacy clauses to collect personal information for secondary use for use in data mining [11]. The written statements of bundled consent may be changed without notice, or some elements outside the privacy policy, or bundled consent could be added to customer agreements to allow data mining in the future [11] [13] [14].

Finally, fair information practices require that when there are any changes to an organisation's

privacy policy the website user should be alerted to this change with information [17] which includes the date of issue and a list of changes made by the organisation to the prior version [18]; and that reasonable notice must be given when ever personal information is to be shared with others [17] [18]. So it is doubtful if e-commerce users express genuine consent to the use of their personal information when they tick on the box that they have read these standard form privacy policies and accept the terms therein. The issue of consent on the internet raises significant privacy concerns with the emergence of new technological challenges.

V. ONLINE PRIVACY VIOLATIONS

The e-commerce users' capacity to exercise autonomy and protect their privacy is further compromised by the use of privacy invasive technologies, the automatic processing of their personal information, and data security risks that threaten privacy. The online activities of Internet and e-commerce users are constantly monitored using electronic surveillance devices for commercial interests [19] [20] [21].

A. Privacy Invasive Technologies

The harvesting of personal information through monitoring and sensing using privacy invasive technologies is pervasive and pose special risks to privacy of individuals [17] [18]. Data surveillance, the most common form used to collect information about e-commerce users without their consent [23] [24]. Information technologies such 'cookies', 'web bugs', [18] [23] [26] and HTTP are key features that allow data collection [1] [23] and enable web pages to be transported between users and a web server. Most of the privacy invasive applications depend upon these technologies. New surveillance technologies such as the RFID chip (Radio-Frequency Identification), and 'behaviour-tracking ad system' is also being used to bring Internet users more relevant advertising and to benefit e-commerce businesses. There have been severe backlash recently from users of social networking websites when it was discovered that two prominent websites such as 'Google', and 'Facebook' have been monitoring and collecting personal information for secondary use without users knowledge, or explicit consent [31]. Other data exchange companies such as 'BlueKai', a California based company, and 'Phorm' (a British company) are involved in tracking online users without notification of data collection. Internet and e-commerce users generally do not know the fate of their personal information that is generated online [27] [28].

B. Automatic processing

Generally e-commerce may have the consented to the collection of their personal information for primary purposes, but e-commerce users do not know if such information will be used for secondary purposes or shared with third parties [18] [30]. The automatic processing and secondary use and disclosure of personal information collected without the consent of individuals through 'data surveillance' also affect individual privacy interests [23] [27]. Automatic processing of personal information allows the aggregation of personal information, identification of individuals, and secondary use of personal information without consent. Cookies are the most common profiling mechanism used on the Internet [18] [27] [29]. Database companies are able to correlate and manipulate the data collected through the process of data matching, 'sentiment analysis', customer profiling, and the creation of digital dossiers [23][26]. Consumer profiles are a major currency in e-commerce [27]. Many database companies are known to sell information about users or provide lists of their customers' e-mail addresses to other direct marketing or telemarketing companies [18] [27]. The processed data in the form of profiles and digital dossiers can be disseminated or can be made accessible easily; it can be transferred quickly from one information system or database to another and across borders with the click of the mouse without the knowledge or consent of the data subject [27]. Some companies readily disseminate the personal information and digital dossiers that have been collected to a host of other entities and sometimes to anyone willing to pay a small fee [27] [30]. The increasing interconnectedness, affordable, fast, on-line systems also enable the building of electronic dossiers [30] [31]. Critical decisions about an individual's status, reputation and credibility either to determine eligibility and suitability for jobs, credit worthiness, and criminal record can readily be made by tapping into digital dossiers [30]. The privacy issue is that profiles expose Internet and e-commerce users to risks of the information being linked to other information such as names, addresses and e-mail addresses making them personally identifiable. Personal information in the digital dossiers is also at risk of being manipulated or used for unintended purposes when it is shared with third parties [27] [32].

C. Data security breach

Online privacy for consumers is also seriously compromised by data security breaches and creates privacy risks for e-commerce users. Insecure systems can give rise to identity fraud if a party acquires a user's identifiers and in particularly identity authenticators [18] [29]. Cyber criminals are ripping data out information from the Internet

and databases [34] [35]. Personal data is at risk of unauthorised access, falling into the wrong hands, misused or becoming a commodity for illegal sale, [18] exposes individuals to identity theft, loss of reputation, confidentiality and potential loss of valuable intellectual property rights [31]. In Australia, the Australian Payments Clearing Association report that the value of online credit card fraud in Australia exceeded $102 million during the period 30 June 2009 – 31July 2010 [33]. Identity theft is becoming increasingly common and is for example the fastest growing crime [35]. Data security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data [18].

Violations of human rights arise from the unlawful collection and storage of personal data, the problems associated with inaccurate personal data, or the abuse, or unauthorised disclosure of such data [20]. The factors discussed above are a major determinant of users disclosing their personal information to e-businesses [15] [16]. It appears that in cyberspace, data collectors such as Internet service providers (ISPs) and the suppliers of content on the web are in the main unregulated in any way under the current privacy provisions.

VI. REGULATION

Currently, almost all fair information practices such as for example under the OECD's Collection Limitation Principle [36]; Directive 95/46/EC [17] and the Asia-Pacific Economic Co-operation (APEC) – Privacy Framework provide for privacy principles [36]. These privacy principles provide for compliance with displaying privacy policies statements; notice of personal information collection, use and/or disclosure; breach notification; access and correction that are viewed as a prerequisite for fair information collection practices. In the Asia Pacific region, APEC's Data Privacy Pathfinder [38] contains general commitments leading to the development of a Cross-Border Privacy Rules (CBPR) system.

In Australia, there is no right to privacy under the common law although a statutory tort of privacy is being mooted [18]. Privacy protection in Australia is a patchwork of federal and state statutory regulation and industry codes of practice and incidental protection at common law arising out to torts, property, contract and criminal law. The primary federal statute for privacy protection that is the *Privacy Act 1988* (Cth) ('*Privacy Act*') National Privacy Principles ("NPPs") [36] have their foundation consumer choice or consent as an essential element. However, the existing legislative structure under the *Privacy Act* appears to give priority to commercial interests in relation to direct marketing and secondary usage. Neither the *Privacy Act* nor the NPPs prohibit bundled consent.

There are currently law reform initiatives at the international, regional and national levels to enhance privacy protection for individuals. For example under the e-Privacy Directive, EU Member States are required to ensure that the storing of information, or the gaining of access to information already stored**,** is only allowed on condition that the data subject concerned has given his or her consent, having been provided with clear and comprehensive information**,** in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing [37]**.** In Australia, the Australian Law Reform Commissions (ALRC) has in its recent report on proposed recommendations to enhance privacy protection [18]. Amongst others it has recommended developing a single set of Privacy Principles; redrafting and updating the structure of the Privacy Act; and addressing the impact of new technologies on privacy; and data security breach notification.

VII. SOLUTIONS

This paper also suggests that there should be more appropriate regulatory response to remove constraints which impede considered decisions about privacy by e-commerce users needs to be in place to protection of personal information in cyberspace. Viewed from the standpoint of individual privacy, legislation should ensure that constraints on the ability to make rational decisions are removed. In relation to e-commerce users, the legislative framework can be satisfied if the user has liberty of action, that is, if the user agrees without duress or coercion. The difficulty of finding and understanding information relating to privacy policies, blanket or bundled consents, the lack of choice whether to accept conditions and the preference give to commercial interests reduces the individual's autonomy to make informed decision making, and to control and consent to the use their personal information. Although it is not possible to ensure that a consumer will act rationally with informed consideration before deciding to waive their privacy rights, the legislature can, at least, legislate to remove constraints preventing informed and rational decision making.

This paper suggests that one of the ways to resolve the problem of consent and choice would be notification prior to collection, use and disclosure should be mandatory. The reason being that notification of data collection, use and disclosure and how such information will used and disclosed include in a standard from privacy policy encourages transparency about data collection and the subsequent handling of personal information. Notification allows individuals to be able to access their personal information and to correct incorrect information held about them; and it also allows

individuals to withhold consent to the collection of personal information for unlawful purposes [18]. Notice allows an autonomous individual the option to decide and make choices whether to share their personal information with others. In addition to notification of collection use and disclosure, mandatory notification of data security breaches alerts customers and ensures that customers and users are able to take timely action to limit risks to their personal information from risk by for example changing their pin number and passwords [18]. Notification of data security breach gain consumer trust and reduced risk to personal information.

Besides regulation there are a range of methods that can be adopted to enhance privacy that involve a combination of approaches and mechanisms that include legislation, technology based enhancing mechanisms, education and business best practice rules.

VIII. CONCLUSION

This paper has examined the significance of privacy for individuals. It argued that autonomy is only truly observed if the e-consumer is able to provide explicit consent and has both choice and the opportunity to make rational and informed decisions. It also argued that consent to the collection, use, and disclosure of personal information should be regarded as instrumental to individual autonomy. This paper examined and identified some of the online privacy problems that arise from the use of privacy invasive technologies by data collectors and its effect on the privacy interests and risks to individuals. This paper has also suggested some solution to the problem to exercising consent and choice. This paper has suggested that any choice regime should provide a simple and easily accessible way for consumers to exercise this choice. It is suggested that the opt-in regimes must require positive action by the consumer to allow the organisation that is collecting and using their personal information [10] [11].

It suggests that appropriate notification prior to data collection; and information provided to e-commerce users if the information collected will be used or shared with a third party or parties. This measure will restore control over personal information and give individuals an opportunity to consent or to withhold consent to the use of their personal information for primary and/or secondary purposes. Such an approach puts a premium on individual choice and privacy but probably at some cost of efficiency for the e-commerce provider.

IX. REFERENCE

[1] Office of the Privacy Commissioner. (2007). *Submission to the Australian Law Reform Commission Review of Privacy Discussion Paper 72'*. Australian Government.

[2] P. M. Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review*, vol. 52, pp. 1609-1702, 1999.

[3] Privacy Commissioner, "Privacy concerns on the up: Annual Report 2009," Office of the Privacy Commissioner, New Zealand, 2009.

[4] Office of the Privacy Commissioner, "Privacy Matters," Australian Government, vol. 1, Issue 4, 2007.

[5] Samuel Warren and Louis Brandeis, "The right to privacy," *Harvard Law Review* vol. 4, pp. 193 – 220, 1890.

[6] A. Westin, *Privacy and Freedom.* New York: Atheneum Publishers, pp. 487, 1967.

[7] B. Rossler, *The Value of Privacy*. Cambridge: Polity Press, 2005.

[8] F. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, pp. 346-402, 1984.

[9] J. W. Penny, "Privacy and the New Virtualism," *Yale Journal of Law & Technology*, vol. 10, pp. 194-250, 2008.

[10] P. Regan, "The role of consent in information privacy protection," Center for Democratic and Technology, 2009.

[11] A. Cavoukian, "Data Mining: Staking a Claim on Your Privacy," Office of the Information and Privacy Commissioner, Ontario, (1998).

[12] R. Clarke, "*e-Contract: A Critical Element of Trust in e-Business,"* presented at the Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, Jun. 2002.

[13] R. Clarke, "*The Effectiveness of Privacy Policy Statements,"* Xamax Consultancy Pty Ltd., 2008.

[14] F. Marotta-Wurgler, **"**Does Disclosure Matter?" *New York University Law and Economics Research Paper*, No. 10, pp. 54, 2010.

[15] Senate Select Committee on Information Technologies. (2000). *Cookie Monsters? Privacy in the information society*. Commonwealth Parliament of Australia.

[16] Out-Law.com, '*Average privacy policies take s 10 minutes to read, research finds'* Out-Law.com, 6 October 2008 [Online]. Available: <http://www.out-law.com/page-9490>.

[17] European Commission. (1995). *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* (hereafter referred to as "Directive 95/46/EC"). Directive 95/46/EC, Article 18

[18] Australian Law Reform Commission (ALRC). (2008, May.). *For Your Information: Australian Privacy Law and* Practice ('ALRC Report 108'). [Online]. Available: http//:www.alrc.gov.au

[19] Australian Communications and Media Authority (ACMA). (2011, Sept.). Growth in sensing and monitoring information driving change in service. ACMA Media Release 89/2011. [Online]. Available: http://www.acma.gov.au/WEB/STANDARD/pc_pc_410135

[20] D. J. Solove, "A Taxonomy of Privacy" *University of Pennsylvania Law Review* vol. 154, No. 3, pp. 477-560, 2006.

[21] Electronic Privacy Information Centre. (2011). *Cookies.* [Online]. Available: http://www.epic.org/privacy/internet/cookies/

[22] A. Cavoukian, "Privacy and the Open Networked Enterprise, Information and Privacy Commissioner, Ontario Canada, 2006.

[23] R. Clarke, "Information Technology and Dataveillance," *Communions of the ACM*, vol. 31, Issue 5, pp. 498-512, 1988.

[24] European Commission. (2009, Nov.). ePrivacy Directive close to enactment: improvements on security breach, cookies and enforcement, and more to come. Reference: EDPS/09/13.

[25] Privacy International, "*PHR2006 – Privacy topics: Electronic commerce,"* Privacy International, 2007 [Online]. Available: http://www.privacyinternational.org/article.shtml

[26] D. J. Solove, *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004.

[27] D. J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," *Southern California Law Review*, vol. 75, pp. 1083-1167, 2002.

[28] Electronic Privacy Information Centre ('EPIC'). (2011, Nov.) *Federal Trade Commission Announces Settlement in EPIC Facebook Privacy Complaint - Social Networking Privacy*. [Online]. Available: http://epic.org/privacy/socialnet/

[29] R. Clarke and A. Maurushat, "The Feasibility of Consumer Device Security," *University of New South Wales Law Research Series*, No. 5, 2009.

[30] D. J. Solove, "The New Vulnerability: Data Security and Personal information" in *SECURING PRIVACY IN THE INTERNET AGE*, Eds. A. Chander, L. Gelman, and M. J. Radin, Stanford University Press, 2005.

[31] Australian Broadcasting Corporation. (2009, Aug.). "Fear in the Fast Lane," Four Corners - ABC.net.au. Available: http://www.abc.net.au/4corners/content/2009/s2658405.htm.

[32] Australian Payments Clearing Association, (2010, Dec.) *Payments Fraud in Australia - Media Release*. [Online]. Available: <http://www.apca.com.au>.

[33] Australian Institute of Criminology, (2011). *Consumer Scams-2010 and 2011*. [Online]. Available: http://www.aic.gov.au/en/publications/current%20serices/rip21-40/rip25.aspx.

[34] Australian Crime Commission, (2011). *Crime Profile Series–Identity Crime - Fact Sheet*. [Online]. Available: http://www.crimecommission.gov.au/sites/default/files/files/identity-crime.pdf

[35] Organisation of Economic Cooperation and Development (OECD). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"). Available: http://www.oecd.org/documentprint/0,3455,en_2649_34255_1815186_1_1_1,00.html

[36] *Privacy Act 1988* (Cth) s 6, and Sch 3 National Privacy Principles (NPPs).

[37] European Union. (2011, May.). *ePrivacy Directive Regulations.* European Commission. Available: http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/data_breach/ePrivacy_databreach_consultation.pdf

[38] Asia-Pacific Economic Co-operation (APEC). (2012, Mar.). *APEC Data Privacy Pathfinder Initiative*. Available:

http://www.ag.gov.au/Privacy/Pages/APEC-Data-Privacy-Pathfinder-Initiative.aspx