International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240
The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)

The Right to Consent and Control Personal Information Processing 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

Consent, information privacy, privacy violations, e-commerce, privacy protection mechanisms.

1 INTRODUCTION

Whilst the internet is undoubtedly beneficial to e-consumers users and other users such as social network users, information technology has affected privacy dramatically [1], [2]. It has made it possible for any person to easily collect personal information about Internet users without their consent. Consumer concerns over the safety of personal information and the violation of an individual's 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]. A recent survey in Europe also indicates that about a quarter of social network users (26 percent) and online shoppers (18 percent) feel that they are not in complete control over their personal data [5]. Internet users are worried that they give away too much personal information and want to be forgotten when there is no legitimate grounds for retaining their personal information [6].

This paper explores the 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. This paper also examines the effects of privacy violations on individual when there is covert collection, automatic processing, and data security risks that arise from such activities. This paper also questions the assumption in most legislation which affects e-commerce users, that consent is sufficient to waive an individual's privacy interests.

This paper proceeds to examines and discusses firstly, the issue of privacy in the e-commerce context of information privacy; secondly, 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 that arise for individuals when there covert collection, use and disclosure of personal information. This paper then 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 in the form of privacy protection mechanisms to the problem of online privacy for individuals.

2 PRIVACY

The important elements of the right to privacy are identified by theorists [7], [8] and [9], as being "the right to be left alone" [7]; and to be anonymous as one of the important elements of privacy. A threat to privacy will be a threat to the integrity of a person [7] 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 [9] and [10]. 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 [9], [10].

Control over information is connected to how individuals want to be seen, to whom they want to be seen, and in what context [8], [9]. 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 [9], [10]. This capacity to control disclosure is seen an element of personal integrity, reputation, human dignity, expectations, autonomy and self determination, happiness and freedom [9], [10], [11]. The individual's ability to control disclosure of facts about themselves is valued as a means of protecting personality rather than property interests [9]. Control includes also the ability to consent, make decisions and choices whether to allow or disallow others into the individual's private space and information about them.

2.1 Consent

Consent is an expression of individual autonomy, and the right for individuals to make decisions about how they will live their lives. According to normal legal principles, consent cannot be effective if the person does not have sufficient knowledge or understanding to consent. 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 [12], [13]. 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 [14], [15].

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 [15]. 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 [13]. 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. Data collectors are also using bundled privacy clauses to collect personal information for secondary use for use in data mining [13]. 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 [13], [15], [16]. So 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 [14], [18].

This paper suggests that the use of bundled consent should be prohibited or closely monitored by regulators so as to not infringe the privacy rights and restrict an individual's right to withdraw consent. The issue of consent on the internet raises significant privacy concerns with the emergence of new technological challenges. 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.

2.2 Choice

A secondary sense in which autonomy is used is that it requires freedom of choice [12], [13]. 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. Choice requires the individual to be a rational consumer making informed and considered decisions and having options in relation to their personal information. 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 which includes the date of issue and a list of changes made by the organisation to the prior version; and that reasonable notice must be given whenever personal information is to be shared with others [19], [20].

In e-commerce, individuals make choices about the use and disclosure or surrender of their personal information for secondary purposes. The options that are available to individuals in cyberspace to collection, use and the sharing their personal information is exercised through the opt-in and opt-out regime. There are 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 [13].

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 [17], [18]. The e-commerce user's ability to exercise autonomy as deliberative choice

is constrained in a number of ways. Firstly, 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. 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. Often internet users also have no alternative but are obliges to give their consent to access services and goods advertised on the Internet. If an individual does not actively select to opt out then he or she is taken to agree by default. Alternatively the box may be ticked as the default state to indicate agreement with the consumer required to 'untick' the box if they do not agree. 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 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. 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 [18].

3. PRIVACY VIOLATIONS

It appears that the e-commerce users' capacity to exercise autonomy and to protect their privacy is further compromised by the automatic processing of personal information, use of privacy invasive technologies, and data security risks.

3.1 Automatic Processing

Automatic processing of personal information allows the aggregation of personal information, identification of individuals, and secondary use of personal information with or without consent. The automatic processing and secondary use and disclosure of personal information collected without the consent of individuals through 'data surveillance' affect individual privacy interests [21], [22], [23]. 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. The harvesting of personal information through monitoring and sensing using privacy invasive technologies is pervasive and poses special risks to privacy of individuals [23].

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 [24], [25]. Cookies are the most common profiling mechanism used on the Internet [24] [25]. Besides the ability to profile e-commerce users, the increasing interconnectedness, affordable, fast, on-line systems also enable the building of electronic dossiers. 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 [22], [25]. 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 [22], [25]. Personal information in the digital dossiers is at risk

of being manipulated or used for unintended purposes when it is shared with third parties [26], [28], [29].

3.2 Privacy Invasive Technologies

The online activities of Internet and e-commerce users are constantly monitored using electronic surveillance devices for commercial interests [25], [26], [27]. Data surveillance, the most common form used to collect information about e-commerce users without their consent. Information technologies such 'cookies', 'web bugs', and HTTP are key features that allow data collection and enable web pages to be transported between users and a web server [1]. Most of the privacy invasive applications depend upon these technologies [1], [20], [25], [26]. 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. 'Cookies' remain invisible and outside the control of the user [30]. The Internet user's control tools do not allow for complete erasure of profiles and data collected even if the user erases such information from their Computers [23] [31].

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. Besides Google and Facebook, 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 [32]. Online privacy for consumers is also seriously compromised by data security breaches and creates privacy risks for e-commerce users [33], [34].

3.3 Data Security Breach

Data security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Besides the infringement of privacy as a human right, personal data is at risk of unauthorised access, falling into the wrong hands, misused or becoming a commodity for illegal sale, [31]. Insecure systems can give rise to identity fraud if a party acquires a user's identifiers and in particularly identity authenticators [31]. Cyber criminals are ripping data out information from the Internet and databases [33], [35]. 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]. Data security breaches expose individuals to identity theft, loss of reputation, confidentiality and potential loss of valuable intellectual property rights [33]. Identity theft is becoming increasingly common and is for example the fastest growing crime [35].

4. PRIVACY PROTECTION IN CYBERSPACE

There is a range of methods that can be adopted to enhance privacy such as a combination of approaches and mechanisms that include legislation, technology based enhancing mechanisms, transparency in information collection, education and business best practice rules. These mechanisms for privacy protection are examined next.

4.1 Regulation

Almost all fair information practices such as for example under the OECD's

Collection Limitation Principle [36]; and European Union's Directive 95/46/EC provide for privacy principles [19], [38], [39], [40]. 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 [36], [19] Similarly, in the Asia-Pacific region, the Asia-Pacific Economic Co-operation (APEC) – Privacy Framework provide for privacy principles [41] provide for personal information protection. APEC's Data Privacy Pathfinder contains general commitments leading to the development of a Cross-Border Privacy Rules (CBPR) system [41]. The EU Directives in particular have been influential but compliance is not mandatory for non EU Member States. Although non-EU countries have adopted similar fair information practices into their national legal frameworks [36], [19] there are various approaches and varying degrees of protection for personal information under national frameworks.

In contrast to EU laws, the Australian privacy framework is considered to be inadequate. The primary federal statute for privacy protection that is the *Privacy Act 1988* (Cth) ('*Privacy Act*') National Privacy Principles ("NPPs") [37] have their foundation consumer choice or consent as an essential element. But there is also no right to privacy under the common law although a statutory tort of privacy is being mooted [20]. 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. 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. Neither the *Privacy Act* nor the NPPs prohibit bundled consent. It also appears that the *Privacy Act* gives priority to commercial interests in relation to direct marketing and secondary usage as the existing legislative structure provide that 'consent' may be 'express consent', or 'implied consent' [37].

At the international level, law reform initiatives are currently focused on enhancing privacy protection. For example the e-Privacy Directive, now requires EU Member States 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 [39]**.** These initiatives have also influenced the Australian Law Reform Commissions (ALRC). The ALRC has amongst others 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 [20]. It is proposed that a single set of privacy rules, compliance and enforcement will strengthen privacy protection for Internet users.

4.2 Other Mechanisms for Privacy Protection

In relation to the problem to exercising consent and choice, it is suggested that any choice regime should provide a simple and easily accessible way for consumers to exercise this choice. This paper suggests that an opt-in regime is a better option than the opt-out regime. It is suggested that the opt-in regimes require positive action by the consumer to allow the organisation that is collecting and using their personal information. It also suggests that simple and effective mechanisms for ecommerce

users and other Internet users to give and withdraw consent must be in place.

Transparency in data collection is a crucial part of data protection. But an average data subject is not always aware of how to use browser settings to reject cookies and often unaware that their online activities are being tracked. Notification encourages transparency about data collection and the subsequent handling of personal information. Appropriate notification prior to data collection; and information provided to e-commerce users such as, if the information collected will be used or shared with a third party or parties, 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. Prior notice to data collection allows an autonomous individual the option to decide and make choices whether to share their personal information with others. Notification with standard privacy clauses attached 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 [19], [20] .

In addition, notification of data security breach gain consumer trust and reduced risk to personal information. 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 [20], [39], [40], [42]. Technological tools establishing privacy preferences besides continuous privacy awareness and education can also be effective in protecting personal information.

5 CONCLUSION

This paper has examined the significance of privacy for individuals as a fundamental human right. 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. 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. 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. Consent to the collection, use, and disclosure of personal information should be regarded as instrumental to individual autonomy.

The proposed reforms to enhance information protection in cyberspace both in Europe and the Asia-Pacific region is aimed to strengthen and give Internet users more control over their personal information, make it easier for individuals to access and improve the quality of information they receive from data collectors about what happens to their personal information, with who their information is shared with, and also to ensure that personal information is protected no matter where it is sent or stored. This paper proposes that 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. For example 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. Viewed from the standpoint of individual privacy, legislation should also ensure that constraints on the ability to make rational decisions are removed. But only time will tell if current reforms initiatives and regulation have been effective in protecting personal information of Internet users in cyberspace.

6 REFERENCE

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

[2] Schwartz, P.M.,: 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, vol. 1, Issue 4, Australian Government (2007).

[5] European Commission: Why do we need an EU data protection reform? (2012) http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[6] Special Eurobarometer 359: Attitudes on Data Protection and Elecronic Indentity in the European Union (2012) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[7] Warren, S., Brandeis, L.: The right to privacy," Harvard Law Review vol. 4, pp. 193 – 220 (1890).

[8] Westin, A.: Privacy and Freedom, pp. 487. New York, Atheneum Publishers (1967).

[9] Rossler, B.,: The Value of Privacy, pp. 1-17. Cambridge, Polity Press, (2005).

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

[11] Penny, J. W.,: Privacy and the New Virtualism, Yale Journal of Law & Technology, vol. 10, pp. 194-250 (2008).

[12] Regan, P.,: The role of consent in information privacy protection, Center for Democratic and Technology (2009).

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

[14] Clarke, R.,: e-Contract: A Critical Element of Trust in e-Business. In: Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia (2002).

[15] Clarke, R.,: The Effectiveness of Privacy Policy Statements, Xamax Consultancy Pty Ltd. (2008).

[16] Marotta-Wurgler, F.,: Does Disclosure Matter?, New York University Law and Economics Research Paper, No. 10, pp. 54 (2010).

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

[18] Out-Law.com: Average privacy policies take s 10 minutes to read, research finds,' Out-Law.com (2008) http://www.out-law.com/page-9490.

[19] European Commission: 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 ("Directive 95/46/EC") (1995).

[20] Australian Law Reform Commission (ALRC): For Your Information: Australian Privacy Law and Practice ('ALRC Report 108') (2008).

[21] Australian Communications and Media Authority (ACMA): Growth in sensing and monitoring information driving change in service, ACMA Media Release 89/2011 (2011).

[22] Solove, D. J.,: A Taxonomy of Privacy, University of Pennsylvania Law Review vol. 154, No. 3, pp. 477-560 (2006).

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

[24] Cavoukian, C.,: Privacy and the Open Networked Enterprise, Information and Privacy Commissioner, Ontario, Canada (2006).

[25] Clarke, R., : Information Technology and Dataveillance, Communions of the ACM, vol. 31, Issue 5, pp. 498-512, (1988).

[26] Privacy International: PHR2006 – Privacy topics: Electronic commerce (2007) http://www.privacyinternational.org/article.shtml

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

[28] Solove, D. J.,: Digital Dossiers and the Dissipation of Fourth Amendment Privacy, Southern California Law Review, vol. 75, pp. 1083-1167 (2002).

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

[30] R. Clarke, R., A. Maurushat, A.,: The Feasibility of Consumer Device Security, University of New South Wales Law Research, Series No. 5 (2009).

[31] Solove, D.J.,: The New Vulnerability: Data Security and Personal information. In : Securing Privacy in the Internet Age, A. Chander, A., Gelman, L., Radin, M. J., (eds.) Stanford University Press (2005).

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

[33] Australian Payments Clearing Association: Payments Fraud in Australia - Media Release (2010) http://www.apca.com.au.

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

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

[36] Organisation of Economic Cooperation and Development (OECD): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) (1980) http://www.oecd.org/documentprint/0,3455,en_2649_34255_1815186_1_1_1,00.html

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

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

[39] European Commission: EU Directive on Privacy and electronic Communications, Article 29 WP Issues Opinion on Cookies in the New ePrivacy Directive (2010).

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

[41] Asia-Pacific Economic Cooperation (APEC): APEC Data Privacy Pathfinder Initiative (2012) http://www.ag.gov.au/Privacy/Pages/APEC-Data-Privacy-Pathfinder-Initiative.aspx

[42] Greenleaf, G.,: Five years of the APEC privacy Framework: Failure or promise? (2008) http://austlii.edu.au/~graham/publications/2008/Greenleaf_ASLI0408.pdf