9-2011

Data Protection Laws and Marketing Practices

Warren B. CHIK
Singapore Management University, warrenchik@smu.edu.sg

Data Protection Laws and Marketing Practices

By Warren B. Chik

Published in Singapore Law Gazette, 2011 September http://www.lawgazette.com.sg/2011-09/

The potential privacy implications of the incorporation of data protection laws in Singapore for unsolicited communications including telemarketing, junk mail and faxes and SPAM are examined in this article.

Data Protection Laws Expected to be Introduced for Singapore in 2012

The efforts to introduce a data protection regime in Singapore have been in the backburner for years, but it appears that the government has done its internal studies and is ready to introduce more comprehensive data protection laws sometime in 2012.[1] This is to bring the Singapore privacy and data protection laws in line with the global benchmark. Legislation will also render adherence and observance mandatory unlike for voluntary codes.[2] This is important as there is little social awareness or recognition of privacy rights in civil society, hence the government has to take the lead in creating awareness and in setting the standards and expectations of protection, especially for the private sector.

The long overdue legislation, according to the then Minister for Information, Communications and the Arts ("MICA") Mr Lui Tuck Yew is to provide baseline standards and to "curb excessive and unnecessary collection of an individual's personal data by businesses, and would include requirements such as obtaining the consent of individuals to disclose their personal information".[3] It is to be expected that the basic requirements set out decades ago in the "OECD Privacy Principles" that have since been transposed into the European Union regional and other national regimes will feature in the legislation.[4]

Timely to Revisit the SPAM Control Act and to Consider Stricter Telemarketing Regulations and Junk Mail and Fax Control Laws

The first line of business by the government should be to set up a watchdog body much like the Privacy Commission in Hong Kong in order for the proposed law to be effective and to provide strong disincentives to non-observance.[5] It should also transfer some of the responsibility for the policing of business practices and to take up complaints from the public. Under the "Accountability Principle", "[a] data controller should be accountable for complying with measures which give effect to the [other privacy] principles".[6] The SPAM Control Act (Cap 311A) places the burden of ensuring compliance with its requirements mainly on the victim in a private civil course of action. This is unsatisfactory given the lack of personal resources.[7]

Another thing that should be done, given the convergence of the subject matter, is for the relevant agencies and for Parliament to seriously look into amending the SPAM Control Act and supplementing it with more comprehensive laws and regulations against other forms of unsolicited commercial messages, especially through telemarketing and junk mail and faxes.[8] These other practices that are becoming more of a nuisance than SPAM are largely currently unregulated except for some industrial guidelines or codes of conduct that do not provide enough privacy for the individual.[9] Telemarketing is especially insidious as it involves the trading of personal information,[10] often cannot be traced (especially when it is made from a private line), (and together with junk mails and faxes) can even result in financial cost/loss to the recipient

and cannot be screened or filtered out (unlike SPAM and online advertisements). The diversified and multi-pronged approach to bombarding society with sales pitches and the increasing use of "push" technology and practices is a serious incursion into personal space and peace. In contrast, some other countries that have stricter laws only allow people to "pull" (ie, solicit, request or permit) advertisements. These proposed laws and regulations can come in the form of an omnibus statute or in specific provisions or Acts covering all forms of unsolicited messages rather than of just the electronic (or even commercial) variety.

In summary, the baseline of protection is currently either too low (ie, the legitimization of SPAM) or non-existent (in the case of other forms of unwanted communications); and the other problem is the lack of deterrence and enforcement.

It is not only a mere preference for Singapore to adopt the stricter regulatory laws to control unsolicited communications. It is a need. There are two bases for this observation. First, the lack of laws against telemarketing and junk mail or faxes as well as the ineffectiveness of the current SPAM Control Act is adversely affecting the overall effectiveness of social media, modern telecommunications, the information-based economy and human productivity (the policy basis).[11] Singapore may also face a restriction of trans-border flow of personal data from other countries and regions (notably the EU) on the basis that we do not substantially observe international privacy and data protection standards that they adhere to in their laws. Second, the OECD Privacy Principles, which are expected to feature in our proposed legislation, mandates stricter guidelines and duties with regard to data collection, storage, use and sharing that will have direct implications for marketers or advertisers and their clients (the legal basis). The mechanics and processes behind the sending of unsolicited communications involves the gathering and handling of personal information, thus the link between data protection and privacy laws on the one hand and laws regulating and restricting unrequested advertisements on the other.[12] [13]

Implications of Data Protection Laws for Unsolicited Communications

A two-pronged approach is key to an effective legal strategy against such practices. An "opt-in" regime that only permits the solicitation or permission for advertisements (direct or indirect and in various forms including deals, newsletters and updates),[14] supplemented by an "opt-out" regime to deal with personal information that is already, prior to the enactment of the new law, used and circulated among businesses, marketers and list sellers as well as to deal with data collected and managed after the new laws come into effect in compliance with the legal and regulatory requirements.

"Opt-in" to advertisements: It must be made clear that I am not calling for a total prohibition of electronic and other forms of advertising. It is unrealistic and does not take into account the social benefits and economic advantages of such practices. However, there needs to be a more balanced approach to conflicting policy interests weighing the opposing social forces. Individuals-Recipients can opt into receiving messages and mail – this is in the Company-Advertisers' interests. In fact, many have the practice of pre-selecting or ticking consent-receipt terms, which although is a dubious form of practice, can be accepted as a compromise – especially since sufficient notice of terms can bind parties to an agreement, even an online one. There are also countries that have successfully enacted and implemented an opt-in regime such as in the EU and Australia.[15]

"Opt-out" from communications: Such a practice will be prospective and will require some effort on the part of the person concerned. It is consistent with the "Individual Participation Principle" that allows a person to find out what personal information a data controller has on himself/herself as well as "to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".[16] It is also a common practice for laws controlling un-request communications

including the current SPAM Control Act (Cap 311A). Opting out should also be made more effective and categorical by allowing for a general opt out from all forms of unwanted communications through any medium. For example, the United States has laws governing unsolicited telemarketing;[17] and the Federal Trade Commission ("FTC") introduced a national "Do Not Call" registry in 2003,[18] which has been relatively successful in implementation.[19] The US also has "anti-junk fax" laws.[20] In order for this to work and in line with the Privacy Principles, telephone calls should be made from disclosed numbers and not unknown calls to allow call-backs and tracing.[21] Telemarketing and junk mail/fax control laws can be very effective as they can often be traced (for potential sanction), largely operate within jurisdiction (due to operational costs and potential clients) and have an additional incentive to comply (every call, mail or fax sent costs money unlike the nominal cost of spamming). Individuals should be able to easily request removal from lists of a company and its affiliates, not just of a particular type of advertisement – otherwise the advertiser can merely take advantage of the loophole and slightly modify advertisements and continue to SPAM them.[22]

Generally, the data protection laws should also require greater transparency (the "Openness Principle"),[23] and adherence by data controllers to the "Collection Limitation Principle",[24] the "Use Limitation Principle"[25] and the "Purpose Specification Principle"[26] that should reduce the abuse in trading of personal information as commodity and improve consumer knowledge and consent. The restrictions on how marketers can gather their mailing lists are currently not sufficiently stringent and the often ambiguous terms regarding the sharing or sale of personal information legitimately obtained is often buried within the fine print of their terms of use or privacy statements. These requirements for transparency and to inform and involve the persons whose data are collected will improve things. Individuals should also have a right to know what information is collected on them and modify it as and when they like and remain in control of their personal information.[27] They should be asked when their information is traded or shared. Perhaps there should not even be an industry in the buying and selling of personal information.[28]

Conclusion

The continued viability and the future of communications technology require an efficient regulation of online advertising and marketing behaviour. It is not a good reason to capitulate to aggressive messaging, and provide too low a threshold for the sending of unsolicited messages on the basis that it is only effective for enforcement within jurisdiction – the truth is that most advertising, especially through land lines and mobile telephony systems are sent from local companies or businesses with a local presence (where there is a market for their products and services). They also tend to be in certain industries – namely, the insurance, property and banking sectors. Something can definitely be done to curb the over-enthusiastic advertiser.

SPAM accounts for up to three-quarters of e-mails sent worldwide, according to sources cited by the Singapore SPAM Control Resource Centre.29 Not only that, SPAM also increases the chance of the spread of virus, and technological/filtering measures are not fool-proof – too low a setting allows SPAM to slip through, too high a setting may divert legitimate messages to the SPAM/junk e-mail folder. The thorough review of data protection and privacy laws is also an opportune time to revamp the laws and regulations in relation to other social nuisances like telemarketing and the practice of cold calling as well as physical junk mail and faxes. The privacy and data protection principles are directly relevant to these issues. The introduction of comprehensive privacy and data protection law is a welcome change and will hopefully deal with the increasing nuisance and problems that unsolicited advertising is posing to society in a way that will improve the rights of the individual. It is hoped that even with a change of Minister after the Cabinet re-shufflement in 2011 following the Singapore Elections, the process will not stall once again.[30]

Warren B. Chik
Asst Prof of Law
Singapore Management University
E-mail: warrenchik@smu.edu.sg

Notes

1 Currently Data Protection is sectoral and limited to specific statutes such as the Banking Act (Cap 19), Official Secrets Act (Cap 213) and the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap 319) where economic interest requires it in the private sector, where information is particularly sensitive (eg, health and financial information) and where it relates to the public sector. Confidential information is also protected under a common law duty of care and the Computer Misuse Act (Cap 50A). It was seven years since it began its review. Leong Wee Kiat, "Finally an End to Private Firms Sharing Your Data?" (*TODAY*, 17 February 2011).

2 The only standard for data protection currently is set under the National Internet Advisory Committee's Generic "Model Data Protection Code for the Private Sector" by the IDA and the National Trust Council which is modelled after internationally recognised standards that was released for private sector and that was available for adoption a decade ago in December 2002. There is scant interest in the Code and little awareness of its existence among the public. See Editors, *Singapore Companies Lag Behind in Data Protection: Accenture* (Enterprise Innovation, 28 April 2010), available at: http://www.enterpriseinnovation.net/content/singapore-companies-lag-behind-data-protection-accenture. There is also no oversight over the standards of other industry-specific self- and co-regulatory codes.

3 See Shamma Iqbal, *Singapore to Introduce Data Protection Law* (Inside Privacy, 13 May 2011), available at: http://www.insideprivacy.com/international/singapore-to-introduce-data-protection-law/, Lim Chong Kin, *Singapore Data Protection Law Expected to be Introduced in 2012*(Drew & Napier Legal Update, 15 February 2011), available at: http://www.drewnapier.com/pdf/150211_LegalUpdate.pdf and Clarice Africa, *Singapore to Introduce Data Protection Regime in 2012* (Asia Pacific futureGOV, 21 February 2011), available at: http://www.futuregov.asia/articles/2011/feb/21/singapore-introduce-data-protection-regime-2012/.

4 See the *Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("*OECD Privacy Principles*"), available at: http://oecdprivacy.org/. These Principles have been substantively adopted by regional and national data protection and privacy laws such as the European Union's Data Protection Directive (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML) and the Hong Kong (Personal Data) Privacy Ordinance (http://www.pcpd.org.hk/). See also, the Privacy of Personal Data in Hong Kong website at: http://www.privacy.com.hk/. 2010 was the 30th Anniversary of the OECD Privacy Guidelines. See the Anniversary Statement at: http://www.oecd.org/document/35/0,3746,en_2649_34255_44488739_1_1_1_1,00.html. See further, the *Asia-Pacific Economic Cooperation Privacy Framework* ("*APEC Privacy Framework*") of 2005, available at: http://publications.apec.org/publication-detail.php?pub_id=390.

5 See the Office of the Privacy Commissioner for Personal Data, Hong Kong website at: http://www.pcpd.org.hk/. The government's review did mention that a Data Protection Council is also expected to be set up to oversee the implementation of the proposed legislation.

6 Para 14, OECD Privacy Principle 8. According to para 62: "Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance". This is especially important for the "Security Safeguards Principle" at para 11, OECD Privacy Principle 5, which requires personal data to be "protected by reasonable security safeguards against such risks as loss or

unauthorised access, destruction, use, modification or disclosure of data". Given the ease of replication and dissemination through electronic and digital means, a lapse in security will also lead to leakage of personal data and information and potentially greater inflow of unsolicited messages from third parties.

7 See eg, Jensen Wee, "Give More Teeth to Anti-SPAM Act" (*Straits Times* Forum, 6 April 2009) for individual's account.

8 They shall collectively be known as "unsolicited" or "unrequested" "communications" or "advertisements".

9 Eg, the Direct Marketing Association ("DMAS") has a code of practice for telemarketing, which allows unsolicited calls, just like the SPAM Control Act allows unsolicited messaging. It is also self-regulating and does not have any sanction for breach of the code. For example, as reported in the news, the limiting of sending of SMS by 10pm by the property agents is not good enough. The SPAM Control Act (Cap 311A) does not extend to all forms of communications such as physical equivalents of junk mail or faxes as well as electronic analogues like cold calls (see s 4(3) of the Act, where a message sent through a voice call that is made using a telephone service is excluded from the definition of an "electronic message"). They are not messages sent in bulk and may not constitute an electronic message (ie, physically delivered junk mail), although they are often commercial in nature. Hence, they are largely unregulated, except perhaps by the industry concerned or aspects of it through specific sector legislation/regulations.

10 Even government owned companies have "lapsed" in this regard. It has been reported that "Mediacorp received a company's offer of 10,000 emails of key Government and ministry officials at a price of S$1,000. Around 10,000 top management executives' personal details were also offered for S$6,000." See *Leong Wee Kiat* at note 1. The security concerns relating to the data kept by the government departments is also an issue. See note 6.

11 The SPAM Control Act is clearly inadequate to protect Singaporeans from unsolicited commercial electronic messages. Personal and anecdotal evidence show that a large amount of messages sent via e-mails and SMS are advertisements – most of which are sent en masse from automatons using marketing lists that are freely traded and exchanged. Another reality is that many people bear with SPAM rather than respond for obvious reasons. Also, not all advertisers adhere to its requirements but yet there seems to be no effective enforcement. The civil cause of action is also not realistic as most do not have the time or bother with the effort of taking one. Thus, a watchdog will be useful in this regard. The government needs to take the lead in enforcement as it is not realistic to expect individuals or civil society groups to do so. The adoption of an "opt out" regime should be revisited. See Warren B. Chik, "Proposed Anti-Spam Legislation Model In Singapore: Are We Losing The War Before Even Starting The Battle?", [2005] 17 *SAcLJ* 747 and Karthik Ashwin Thiagarajan, "The Spam Control Act 2007", [2007] 2 *SJLS* 361. See also, Tan Wei Ming, "Protecting Personal Information Takes Good Governance" (*Business Times*, 2 April 2009). "Good governance is key to managing this substantial amount of information flow and also to safeguard against any misuse of personal data. Inadequate governance, as seen from recent financial troubles, can cause tremendous uncertainty and fear. A sound governance model, when adequately enforced, will give people greater confidence to communicate and transact, whether in the physical or online world." *Ibid*.

12 See "Written Answers to Questions for Oral Answer Not Answered by 3.00 pm: Law on Protection of Privacy Of Individuals and Personal Data" (*Hansard*, 19 January 2009), available at: http://stngiam.wordpress.com/hansard-19-january-2009/.

13 Although currently the main problem is with commercial or business-related messages, non-commercial communications should also be noted in case it also develops into a problem. Moreover, the OECD Privacy Principles do not relate to the objectives of the "data controller" and hence is of wider application than the subject matter of this paper.

14 Online and physical registration and subscription forms can provide for, and even "pre-check" these options provided that sufficient notice, in line with contract law requirements, are met.

15 See eg, the EU Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (Article 13 on unsolicited communications: http://eur-lex.europa.eu/pri/ en/oj/dat/2002/ l_201/l_20120020731en00370047.pdf). See also, EU Directive 2003/58/EC http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do? uri=CELEX:32003L0058:EN:HTML (amending Council Directive 68/151/EEC http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do? uri=CELEX:31968L0151:EN:HTML).

16 Para 13, OECD Privacy Principle 7. See further, the Australian SPAM Act No 129 of 2003 (Cth.) (http://www.acma.gov.au) and the proposed Canadian Fighting Internet and Wireless SPAM Act, Bill C.28 (http://www.parl.gc.ca/HousePublications/Publication.aspx?DocID=4547728; legislative summary at: http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c28-e.pdf). Contrast the approach to the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act (15 U.S.C. §7701, *et. seq.* (2003)) that also has an "opt-out" approach like Singapore.

17 The FTC issued a set of Telemarketing Sales Rule ("TSR") in 1995. On January 2003, the US Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108 (2000)), which significantly amended the TSR (16 C.F.R. § 310 (2003)). A consumer may also stop a telemarketer from calling again on behalf of a particular seller if he/she informs the telemarketer that he does not wish to receive calls on behalf of that seller. *Ibid* at § 310.4(b)(iii)(B)(i). That amendment also provided for the "Do Not Call" registry.

18 The National Do Not Call Registry has a website online that administers the registry at: https://www.donotcall.gov/. It also allows complaints to be made online.

19 FTC Press Release, "Over 55 Million Telephone Numbers Registered – Only 150,000 Complaints in 2003" (13 February 2004), available at: http://www.ftc.gov/opa/2004/02/dncstats0204.shtm. This was according to statistics collected from a Harris Interactive Survey.

20 The Junk Fax Prevention Act of 2005, Pub. L. No. 109-21, 119 Stat. 359 (codified at 47 U.S.C.A § 227 (Supp. 2005)).

21 Eg, the TSR also, among other things, require a telemarketer to provide the consumer's telephone caller identification service with the telemarketer's phone number and, if possible, the telemarketers company name. 16 C.F.R. §.310.4(a)(7). Similarly, junk mail and faxes should contain contact details and information relating to the sender.

22 Moreover, the SPAM Control Act has serious gaps. For instance, it does not require the sender of an SMS to provide the company name, confirm cancellation across related sales agents/companies and products/services, and so on. It also does not deal with the sale and use of external phone number databases and fails to apply the same requirements (eg, unsubscribe option) to telemarketing. See Lim Kok Liang, "Loopholes in SPAM Control Act"(*Straits Times*, 12 June 2011).

23 Para 12, OECD Privacy Principle 6: "There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller." According to para 57, this Principle may be viewed as a prerequisite for the "Individual Participation Principle" in order for the latter to be effective. Hence, "it must be possible in practice to acquire information about the collection, storage or use of personal data … The reference to means, which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost".

24 Para 7, OECD Privacy Principle 1: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data

subject". Para 50 explains that para 7 "deals with two issues, viz: (a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) requirements concerning data collection methods".

25 Para 10, OECD Privacy Principle 4: "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law". Para 55 explains that the Principle "deals with uses of different kinds, **including disclosure**, which involve deviations from specified purposes". (Emphasis added).

26 Para 9, OECD Privacy Principle 3: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose".

27 See, note 16.

28 The government review did note that it would be in Singapore's overall interests to have a data protection regime to protect the individual's personal data against unauthorised use and **disclosure for profit**.

29 Citing data from MessageLabs, an e-mail security and management company, as much as 73 per cent (see http://www.spamcontrol.org.sg/). As an aside, data protection and privacy laws and the relevant authority will need to address other prevalent socio-economic practices like cyber-vigilantism (STOMP, RazorTV), especially in an increasingly connected and urbanized society.

30 See, Vivian Yeo, "Singapore Data Protection Law Stalls" (ZDNet Asia, 25 August 2010), available at: http://www.zdnet.com.au/singapore-data-protection-law-s talls-339305495.htm. The current Minister of MICA is Mr. Yaacob Ibrahim.