Consent - the weakest link in online privacy protection

Svantesson, Dan Jerker B

Published in:
Internet Law Bulletin

Internet Law
Bulletin

Consent — the weakest link in online privacy protection[1]

Dr Dan Jerker B. Svantesson *BOND UNIVERSITY*

Having carried out an assessment of the major weaknesses Australia's law contain in relation to the protection of e-consumers,[2] it has become clear to the author that consent is a crucially important weak spot with far-reaching implications. While it affects a range of areas, the focus here is placed on its impact within privacy law.

Introduction

The relevance of the concept of consent is typically such that consent works like a miracle cure for any alleged privacy violation. If a data controller has obtained the data subjects' consent, it may, for example, use and/or disclose personal data it otherwise would not be entitled to use and/or disclose.[3] Further, it may transfer personal data to a third country where such a transfer would not otherwise be allowed.[4]

Despite its central position in Australian privacy law, legitimate questions have been raised for years regarding the appropriateness of how consent is gained from data subjects.

Focusing on Australian privacy law, this article argues that the current approach taken to consent is unworkable, and that the problems with the concept of consent are amplified in the Internet context. It then proposes an alternative.

What is consent?

There is extensive literature on the concept of consent. This is hardly surprising bearing in mind its central position in several areas of law, including medical law, criminal law and privacy law.

For our purposes here, it suffices to refer to how the concept of consent is applied within Australia's Privacy Act 1988 (Cth). While the Act itself merely makes clear that the concept includes both express and implied consent, Guidelines issued by the Office of the Federal Privacy Commissioner provide more information:

> Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. Consent is invalid if there is extreme pressure or coercion.[5]

The problems

Looking at the concept of consent from a regulator's or a privacy advocate's perspective, the problem is that consent can easily be obtained and works like a magic cure for even the most serious privacy violation. In other words, consent — while virtually meaningless as a procedural protective function — thwarts the protection afforded by substantive privacy law.

Looked at from the perspective of a business operator, the problem with consent is that it may be costly to obtain and difficult to keep track of, leading to additional operational costs.

Combining these two observations, the author concludes that the consent framework found in privacy regulations around the world is costly for business and has the effect of negating the positive effect of substantive privacy laws.

The possible solutions

The most obvious solution would be to re-define the meaning of consent to something more appropriate. At a minimum any such definition should specify that valid consent in the privacy setting must be:

1. Sufficiently informed;
2. Clearly identifiable;
3. Given freely; and
4. Retractable and preferably variable.

The second and the fourth of these requirements are relatively easily dealt with. Consent must be identifiable in the sense that the data controller must be able to point to some particular express or implied indication of consent. The main problem with this arises where the data subject is made to consent to a diverse range of matters as a package, rather than given the chance to consent to some things but not others. Further, consent must be retractable so as to give the data subject the

chance to change her/his mind (obviously such a change of mind may come with consequences such as the data controller ceasing to provide a particular service as long as such matters are specified at the outset).

The application of the first and the third requirements present greater challenges. Assessing exactly what is required for consent to be sufficiently informed will never be an easy task; particularly as it varies depending on what the consent relates to. However, the author suggests that, for consent to be sufficiently informed to be valid, the data subject must, for example, be informed of:

- details about what they are consenting to such as to whom the data may be transferred and under which circumstances such a transfer may take place, the purposes for which the data will be used, and in the case of cross-border data transfers, the country or countries which are the destination(s) of the transfer; and
- generally what are the likely implications of consenting to the use, disclosure and/or transfer.

Also, assessing whether consent was given freely may be difficult in some cases as many instances of a data subject consenting to a particular type of data processing involve the data subject being presented with a "take it or leave it" style choice.

Taking account of the difficulties associated with ensuring that consent is sufficiently informed, clearly identifiable and given freely, and bearing in mind the operational costs associated with collecting and tracking consent, it may be that an alternative must be sought.

One such alternative would be to steer away completely from a consent-focused regulation to a regulatory model with a clearer and firmer definition of what type of data processing is allowed and what type of data processing is not allowed. In other words, as long as the regulation is sufficiently protective of the data subjects' needs, there would be no need for the data subject to consent to the processing. The problem with this approach is obvious; to avoid completely stifling creative data processing practices, such a regulatory model would need to either predict the future or be drafted in such general terms that it could not possibly provide the guidance needed.

A more suitable approach would be for privacy advocates, and more importantly, regulators such as the various data protection authorities, to make better use of existing abuse regulation found in general consumer protection law to assess whether the consent given in a particular instance should be accepted. That way, we can keep the consent-focused regulatory model of today, but ensure that it is applied in a more meaningful manner.

Like the laws of many other jurisdictions, Australian law contains a range of consumer protection provisions that could either be applied directly to assessing whether the consent given in a particular instance should be binding upon the data subject or not. For example, s 51AB of the Trade Practices Act 1974 (Cth) states, in its first sub-section, that: "A corporation shall not, in trade or commerce, in connection with the supply or possible supply of goods or services to a person, engage in conduct that is, in all the circumstances, unconscionable".

This provision could be used to address those instances where the data subjects consent was not given freely, or was not sufficiently informed. After all, in such situations, it would be unconscionable for the data controller to rely on the consent given.

While this provision has its limitations, the absolute majority of instances in which a data subject consents to data processing involve the data controller supplying goods or services to the data subject. Further, as the reference to "corporations" is not restricted by the enormously wide exemptions placed on the application of the Privacy Act (eg that Act excludes small businesses) this provision can be used where the Privacy Act does not even apply.

Another example of general consumer protection legislation that may prove useful in providing guidance on the issue of what constitutes valid consent is found in the Trade Practices Act's regulation of unfair contracts provisions. Inspired by the European Union's useful Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Australia has finally introduced similar provisions dealing with unfair contracts.

This recent amendment to the Trade Practices Act 1974 (Cth) makes clear that, where an individual acquires goods or services predominantly for personal, domestic or household use or consumption, clauses of a standard form contract are void if they are unfair.[6]

In assessing whether or not such clauses are unfair, attention is given to matters such as the extent to which the term is transparent.[7] Further, a term is unfair if:

(a) it would cause a significant imbalance in the parties' rights and obligations arising under the contract; and
(b) it is not reasonably necessary in order to protect the legitimate interests of the party who would be advantaged by the term; and
(c) it would cause detriment (whether financial or otherwise) to a party if it were to be applied or relied on.[8]

Overly broad contractual provisions allowing the data controller to, for example, use or disclose the data in unspecific manners would certainly seem to fit squarely within this provision.

Concluding remarks

Summarising the above, our rather sad conclusion is that the concept of consent — so central to privacy regulation around the world — simply does not work. It makes sense in theory, but the practical application of the concept illuminates its flaws. The consent framework found in privacy regulations around the world is costly for business and has the effect of negating the positive effect of substantive privacy laws.

In light of this, the author has argued that it is time to re-visit and re-design the concept of consent. Preferably this should be done *de novo* and the author has suggested some parameters for a "new" definition of consent. As an alternative, the author has suggested that, the very least that should be done is for various data, and consumer, protection authorities to make better use of general consumer protection provisions that impact on consent. For Australia, that would also require the Australian Competition and Consumer Commission (ACCC) to start taking a greater interest in privacy.

While such a development doubtlessly involves a degree of overlap between the activities of several governmental bodies, it must be recognised that privacy lies at the heart of consumer protection.

Dr. Dan Jerker B. Svantesson
Associate Professor, Faculty of Law,
Bond University.

Footnotes

1. Research for this paper was funded by a generous grant from the. auDA Foundation.
2. Research project carried out together with Dr Roger Clarke, financed by the. auDA Foundation. The project is currently being finalised and applied the model outlined in Dan Svantesson & Roger Clarke, "A best practice model for e-consumer protection", 26(1) Computer Law & Security Review, 31–37.
3. Privacy Act 1988 (Cth), NPP 2.1(b).
4. Privacy Act 1988 (Cth), NPP 9(b).
5. Office of the Federal Privacy Commissioner, Guidelines to the National Privacy Principles (September, 2001), at 22.
6. Trade Practices Act 1974 (Cth), Sch 2, Pt 2, s 2.
7. Trade Practices Act 1974 (Cth), Sch 2, Pt 2, s 3(2).
8. Trade Practices Act 1974 (Cth), Sch 2, Pt 2, s 3(1).