

Bond University
Research Repository



Information management, customer trust and the law - the importance of a “privacy strategy” in e-commerce

Svantesson, Dan Jerker B

Published in:
Internet Law Bulletin

Published: 01/01/2010

Document Version:
Publisher's PDF, also known as Version of record

Licence:
Other

[Link to publication in Bond University research repository.](#)

Recommended citation(APA):

Svantesson, D. J. B. (2010). Information management, customer trust and the law - the importance of a “privacy strategy” in e-commerce. *Internet Law Bulletin*, 13(7&8), 151-152.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

For more information, or if you believe that this document breaches copyright, please contact the Bond University research repository coordinator.

Information management, customer trust and the law — the importance of a “privacy strategy” in e-commerce

Dr Dan Svantesson¹ EDGE LEGAL

Personal information is an important resource in all business activities, and how a business deals with that resource affects how customers view that business; it also has serious legal implications. Yet many businesses continue to operate without a “privacy strategy”. Indeed, many business leaders have never stopped to consider the interaction between information management, customer trust, privacy and the law.

This article argues that businesses in the e-commerce arena are particularly well-advised in having a privacy strategy. It also discusses how such a strategy is to be constructed and gives practical advice on what to consider in drafting a privacy strategy.

Who is affected?

In our modern society, information is a key resource for virtually all businesses. This is particularly true for those businesses that operate wholly or partly in the e-commerce arena. Some of the information businesses collect, use, store and/or disclose, will be personal in nature. In its current version, the Australian Privacy Act 1988 (Cth), defines “personal information” as:

Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

This definition gives a broad meaning to the term “personal information”. However, the Privacy Act is currently very limited in its scope of application. For example, it typically does not apply to small businesses — that is, a business with an annual turnover of less than \$3,000,000.

Yet, those businesses that are not regulated by the Privacy Act also need to take privacy seriously since there is a clear link between customer trust and business profit. Where a business takes appropriate steps to safeguard its customers’ privacy, trust is created — trust that can be translated into profit.

Trust is something that e-commerce operators have been lacking throughout the history of e-commerce, not

least to the anonymous nature of internet communications and due to the short lifespan of many online businesses.

In light of that, all businesses, and particularly e-commerce businesses, need to have a privacy strategy that:

- 1) takes into account the industry in which the business is operating;
- 2) is in line with the business’s goals; and
- 3) is sensitive to the regulatory environment in which the business operates.

Once a privacy strategy has been formulated, the business should put in place a privacy policy, accessible to customers, employees, and others that the business comes into contact with, that operates to support the privacy strategy.

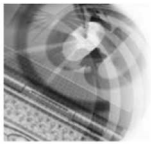
What needs to be considered in a “privacy strategy”?

The exact content of a privacy strategy will vary from business to business. However, generally speaking, an appropriate privacy strategy will assess how privacy impacts on the business. This includes:

- 1) What aspects of the business’s activities are (or could be) restricted or otherwise negatively affected by privacy concerns?
- 2) What aspects of the business’s activities are (or could be) enhanced or otherwise positively affected by good privacy practises?

A privacy strategy should also answer the following 10 questions:

- 1) What types of personal information does the business collect, store, use and disclose?
- 2) How does the business collect, store, use and disclose personal information?
- 3) In what circumstances, if any, does the business transfer personal information overseas?



- 4) What steps does the business take to safeguard the accuracy, integrity and security of the personal information?
- 5) To what extent is the business's handling of personal information regulated by the law?
- 6) Will the business collect personal information only where absolutely necessary, or are there broader collection interests?
- 7) How will the business deal with personal information it no longer has any need for?
- 8) Who within the business will monitor privacy issues?
- 9) What are the areas of risk in the business's handling of personal information?
- 10) How will the business communicate its privacy strategy to employees, customers and other relevant parties?

Obviously, it is also useful for the privacy strategy to contain deliverables and a timetable for achieving the objectives of the privacy strategy.

Concluding remarks

Privacy was once the exclusive concern of human rights activists. However, today that has changed, and as is evidenced by how most major businesses approach privacy, it is now just as much of a concern in the corporate world.

Furthermore, with a series of spectacular privacy catastrophes gaining widespread media attention, consumers (particularly e-consumers) are becoming increasingly concerned, and savvy, about their privacy. This means that businesses need to take greater steps to gain their trust so as to ensure they can obtain accurate and useful information from their customers.

The key problem is that — to the extent that they have considered the impact of privacy at all — many small and medium size businesses still only see privacy as a risk. A business with a well drafted privacy strategy will not only be able to minimise the risk that poor privacy practises may pose, but turn good privacy practises into an opportunity to improve customer trust and profitability.

Dr Dan Svantesson,
Consultant,
Edge Legal.

Footnotes

1. Consultant (Edge Legal), Associate Professor (Faculty of Law Bond University), and Vice-Chair (Australian Privacy Foundation). The article is written as consultant for Edge Legal. The views expressed are the author's alone.