Cloud Computing Consumer Protocol

Submission by the Australian Communications Consumer Action Network to the Australian Computer Society

16 August 2013

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation
Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact

Steven Robertson,
Policy officer

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

1. Executive Summary

ACCAN welcomes the opportunity to comment on the Australian Computer Society's discussion paper on the Cloud Computing Consumer Protocol. We recently prepared a list of cloud consumer principles,[1] which we are pleased to note is referenced in the ACS discussion paper. Our interest in this topic is in protecting the rights of cloud consumers, including both individuals and small businesses (the latter in their roles as consumers of cloud services).

We are concerned that the Government's response to the consumer issues arising from cloud computing has been to recommend a voluntary protocol that will apparently call for cloud service providers to provide information to consumers while requiring little substantive action. It appears to us such a protocol cannot succeed in achieving a number of the stated aims, in particular:

- Adequate protection for consumers of cloud services;
- Open, honest and fair dealings between cloud service providers and consumers; and
- Adequate privacy protection.

Providing consumer information about services is a relatively straightforward response to consumer concerns, but when used in place of binding and enforceable requirements this approach ultimately results in reduced consumer protections and reduced consumer confidence about these services.

Our submission outlines our concerns with the current proposal in greater detail, and suggests some mechanisms which might be used to ensure that the voluntary protocol is as strong as possible. We stress, however, that even a strong voluntary protocol cannot offer the same range of benefits that proper binding regulations can offer, and that the existence of a voluntary protocol should not be taken as a reason to take no further future action in this area.

The recommendations made in this submission are as follows:

Recommendation 1: In describing cloud services, the language used should be focused on the practical risks and benefits of cloud services, rather than more abstract definitions of cloud services.
Recommendation 2: The protocol must require signatories to meet consumer-friendly standards, rather than simply to disclose information.
Recommendation 3: In developing the protocol, there must be recognition of consumer concerns about cloud services that go beyond privacy, security and jurisdictional issues.
Recommendation 4: The protocol should recognise the specific privacy and security concerns of consumers. Specific issues may include the use of personal information for advertising purposes, and security of data from a range of parties, including from unauthorised third parties, law enforcement organisations and the providers themselves.
Recommendation 5: The protocol should address the specific data handling concerns of SMEs, which may differ from concerns of individual consumers.

[1] ACCAN, *What consumers need from cloud computing*, 2012, <http://accan.org.au/files/Submissions/FINAL_cloud_computing_position_statement.pdf>.

Recommendation 6: The protocol should require signatories to undertake to honour the terms and conditions of a consumer contract for the duration of the contract.
Recommendation 7: In developing the protocol, the focus should be on reducing consumer risks and harms rather than on overcoming 'barriers'.
Recommendation 8: The protocol must require signatories to participate in a complaints process that can deliver outcomes for consumers.
Recommendation 9: Dispute resolution should be attempted in the first instance by internal dispute resolution processes. An independent external dispute resolution service must be available for consumers who are not satisfied by the result of internal dispute resolution. Both dispute resolution mechanisms should be available at no cost to the consumer.
Recommendation 10: The protocol should require that reports of the outcomes of complaint processes be published. Reports should be anonymised to protect the complainant.
Recommendation 11: There should be clear identification of signatories that have been directed to update their policies or that have been withdrawn from the register as a result of a complaint.
Recommendation 12: Regular audits should be conducted to ensure that signatories comply with the protocol, rather than waiting for a complaint. Results of these audits must be made publicly available.
Recommendation 13: The protocol should specify the nature, powers and composition of a governing body responsible for managing the protocol.
Recommendation 14: The governing body should include at least one consumer representative.
Recommendation 15: A list of signatories to the protocol must be maintained on a public website.
Recommendation 16: The list of signatories must be maintained to ensure that the information is up to date.
Recommendation 17: Cloud providers that falsely claim to be signatories must be clearly identified in a public list.
Recommendation 18: There should be regular and open reporting of the operation of the protocol.
Recommendation 19: Regular reviews of the protocol should be conducted, with a range of stakeholders consulted.

2. Responses to the ACS discussion paper

2.1. Question 1. Do you believe a voluntary protocol in which cloud suppliers provide undertakings and information about their services would improve confidence in the market and increase the adoption and take-up of cloud computing services?

ACCAN does not believe that a voluntary protocol—in particular one which relies on providing information to consumers as a substitute for substantive consumer protections—is an appropriate response to low consumer confidence in cloud computing services. We are deeply concerned about the direction suggested in the discussion paper.

Our concerns about the voluntary nature of the protocol are as follows:

- For consumers and small businesses to benefit from the protocol, it will be necessary to ensure that the overwhelming majority of providers sign the protocol. However, there is no reason to expect that significant numbers of cloud providers will sign the protocol. In order for market forces or concerns about reputation and consumer perception to drive cloud providers to sign the protocol, there will need to be both sufficient numbers of signatories that failure to sign is seen as a severe shortcoming, and enough force in the protocol that consumers will prefer a service provided by a signatory over a cheaper service provided by a non-signatory. Given that other voluntary codes frequently have low (or unpublished) numbers of signatories, there is no reason to think a critical mass will be achieved.
- Even where a provider does sign the protocol, any compliance actions will necessarily be limited to recommendations, with no real enforcement possible beyond publishing an account of any violations of the protocol. While the presence of a logo on a provider's website might provide consumers with a sense of confidence about the provider, they will in fact have no greater protection than had they chosen a non-signatory as their provider.
- There is a large and growing number of voluntary industry codes already in existence, many of which appear relevant to cloud providers, but few of which have been taken up by providers of any services. The result is a tangle of overlapping industry codes resulting in unclear consumer protections and consumer confusion about whether a particular code (i) applies to their case and (ii) has been signed by their service provider.[2] For small business users, the large number of codes makes it difficult to determine whether using a particular service provider will be consistent with their compliance requirements.

Additionally, we are concerned that ACS appears to be considering the New Zealand CloudCode as a model for the protocol, which suggests that the protocol will attempt to respond to consumer concerns about cloud computing services simply by requiring providers to disclose information to consumers. This approach may have appeal to industry as a relatively cheap way of addressing consumer concerns, but disclosures are not a suitable method of protecting consumers:

- Consumers are already presented with large volumes of information, whether this is in the terms and conditions of a service or in mandatory disclosures under industry codes. This information is often impenetrable to non-experts, and it is unrealistic to expect that a

[2] Cyberspace Law and Policy Centre, *Drowning in codes: an analysis of codes of conduct applying to online activity in Australia*, March 2012, <http://cyberlawcentre.org/onlinecodes/report.pdf>.

consumer will read and understand this information. Increasing the amount of information given to consumers only exacerbates these problems.

- Consumer protection requires that certain standards are met. If a protocol simply requires a provider to inform the consumer of the systems the provider has in place, then the protocol does nothing to ensure that those systems meet the required standards.[3]
- A protocol which primarily requires disclosure cannot provide useful consumer complaint and redress mechanisms. A complaint under such a protocol will necessarily be based on a provider failing to make the required disclosure, not on a provider failing to provide the necessary standards of service.

We note at the outset that both the DBCDE's National Cloud Computing Strategy and the discussion paper appear to view the question of cloud uptake largely in terms of SMEs, while individual consumers receive only brief mentions. This is a dangerous oversight. While SMEs will be significant consumers of cloud services, individuals will also consume cloud services either directly or indirectly, as customers of SMEs using cloud services. Individuals and SMEs will each have distinct concerns about cloud use, and by effectively ignoring the concerns of individuals there is a risk that the foundation of the cloud market will be weakened.

2.2. Question 2a. If you are a potential user of cloud services, do you now have a better understanding of cloud computing and its benefits for your business or operations? What further information do you need to feel confident in deciding to adopt cloud services into your business?

For many individuals and small business consumers, terms such as 'elasticity', 'increased scalability', 'overcoming barriers to capital and expertise', 'mobility', or 'a platform for growth' are unlikely to convey any real benefits that they might gain from cloud computing. Even where consumers recognise that elasticity, scalability, etc. are useful qualities to have in ICT systems, these terms are set out in the discussion paper in so abstract a way that many consumers may not be able to relate the benefits to their own circumstances.

Given that the purpose of the protocol is to encourage consumers to take up cloud services, we suggest that an effort must be made to identify the needs of consumers as the consumers themselves see them, and in terms that consumers use when considering the ICT problems they face. This may include, for instance, 'reliability', 'value', 'safe', 'simpler', and 'compliant'. ACCAN does not question whether a well-designed cloud service could provide all these qualities, but we are concerned that terms used by expert commentators (such as NIST) and by cloud salespeople may not be the appropriate terms for addressing consumer concerns about cloud services.

> **Recommendation 1:** In describing cloud services, the language used should be focused on the practical risks and benefits of cloud services, rather than more abstract definitions of cloud services.

[3] This concern cannot be satisfactorily addressed by relying on market forces to eliminate the providers that fail to meet the necessary standards. Market forces might address the problem if consumers were fully informed and free to choose from a range of providers. In reality, consumers cannot be expected to be fully informed while they are being presented with ever-increasing loads of information about services, and consumers' choice will generally be limited to a handful of major providers, all of which may fail to meet the necessary standards of consumer protection.

2.3. Question 3. If you are a potential or current user of cloud services, do you have other concerns about cloud computing that have not been outlined in this section? What are they?

Question 4. Are there other disclosures from cloud vendors that have not been outlined in this section? What are they?

As noted above, ACCAN is concerned that the protocol appears to be directed towards disclosure of information rather than on substantive consumer protections. While the discussion paper correctly identifies many of the consumer protection issues in cloud computing, the proposed method for addressing consumer concerns is simply to tell consumers what the terms of service are, rather than to set out acceptable terms of service. For example, the discussion paper notes that:

> The ownership of data and information supplied by the client to the service provider needs to be clearly disclosed, to ensure the rights to use the information are clearly understood. This will help identify who owns client data, and data generated by the service provision.[4]

However, a provider could easily satisfy this requirement simply by informing the consumer that the provider takes ownership of any data placed onto a cloud system, even though such a condition would be hostile to consumers. Excessive amounts of information may also lead to confusion, and ultimately lead consumers to reject services.[5]

Instead of mere disclosures, the protocol should require signatories to meet certain substantive consumer protection requirements. This would help to ensure that consumer needs are being met, which would in turn increase consumer confidence in cloud computing.

> **Recommendation 2:** The protocol must require signatories to meet consumer-friendly standards, rather than simply to disclose information.

ACCAN recently compiled a list of such requirements, which we note are referred to in the discussion paper. These requirements include:

- Accessibility of cloud services for people with disabilities;
- Interoperability between different cloud services;
- Ownership of data by the consumer;
- Privacy and protection of personal information;
- Redress mechanisms providing simple and low-cost avenues for complaints;
- Security of the service and the information stored or processed by that service;
- Simplicity of the service and its terms and conditions; and
- Transparency about the jurisdiction and laws that apply to the cloud service.

---

[4] ACS discussion paper, p 12.
[5] Deakin University and ACCAN, *Seeking straight answers: consumer decision-making in telecommunications*, 2011, <http://accan.org.au/index.php/publications/reports/general/365-seeking-straight-answers-consumer-decision-making->.

While many of these issues are identified in the discussion paper, they are not included in any detail in the list of barriers to cloud uptake by SMEs, with the exception of privacy, security and jurisdictional issues. While privacy, security and jurisdiction are certainly important and difficult matters of cloud policy, they are not the only factors that will limit uptake of cloud services. It would be useful for discussions during the development of the protocol to recognise that other issues (such as interoperability and vendor lock-in) will also be a concern to many consumers (both individuals and SMEs) so that they may be given due consideration.

> **Recommendation 3:** In developing the protocol, there must be recognition of consumer concerns about cloud services that go beyond privacy, security and jurisdictional issues.

Even within privacy and security, there are issues that are likely to cause concern for many consumers but which are not addressed in this section:

- A common business model among consumer-grade cloud service providers is to provide a service at little or no cost, and to instead generate revenue by providing targeted advertising services. The discussion of barriers in this section appears to focus on privacy and security in terms of preventing unauthorised disclosures of personal information to third parties and preventing unauthorised access to personal information. A 2013 report from the ACMA noted that many people are concerned about the use of their personal information for marketing purposes,[6] suggesting that this behaviour by providers may be limiting the uptake of cloud services.
- For some small businesses, uncertainty about their own compliance requirements may make it more difficult to determine whether using a cloud service is compatible with those requirements. This concern is only increased by the possibility of the small business exemption to the *Privacy Act 1988* being removed in the future, as recommended in the 2008 ALRC report into privacy.[7]
- For both individual and small business consumers, the complexity of cloud regulation and uncertainty about whether a particular cloud provider adequately addresses privacy and security concerns (along with the other issues identified above) are additional grounds for concern. Even where a provider claims to provide some protection—non-disclosure to third parties, for instance—it may not be clear whether that claim has any binding force, whether the provider will consider some situations (such as disclosure to advertising partners) fall outside the scope of that claim, or whether the consumer has any redress if the provider fails to live up to their claim. A rigorous auditing process to establish that a particular provider meets clearly specified compliance requirements may help to reduce these concerns, but it is not clear that a voluntary protocol can do so.

> **Recommendation 4:** The protocol should recognise the specific privacy and security concerns of consumers. Specific issues may include the use of personal information for advertising purposes, and security of data from a range of parties, including from unauthorised third parties, law enforcement organisations and the providers themselves.

---

[6] ACMA, *Privacy and personal data*, Emerging issues in media and communications, occasional paper 4, June 2013, <http://www.acma.gov.au/~/media/Regulatory%20Frameworks/pdf/Privacy%20and%20digital%20data_Final%20pdf.pdf>.
[7] Australian Law Reform Commission, *For your information: Australian privacy law and practice*, report 108, chapter 39, 2008, <http://www.alrc.gov.au/publications/report-108>.

We also note that many SME consumers will have concerns about the use of their data that go beyond privacy. While privacy is a right of individuals, many elements of privacy—particularly non-disclosure—will be of concern to SMEs. A small business engaged in research and development, for example, may have an interest in ensuring that its data is not disclosed by a cloud provider to third parties without authorisation. While this is a matter of non-disclosure, it is not a question of privacy per se.

> **Recommendation 5:** The protocol should address the specific data handling concerns of SMEs, which may differ from concerns of individual consumers.

Many individual and SME consumers may also be reluctant to commit to a cloud service that may change critical terms and conditions during the service—increasing the service price or reducing cloud storage space after a few months, for instance. The protocol should require providers to undertake to honour terms and conditions for the duration of a consumer's contract or, at a minimum, to provide consumers with a right to terminate their contract without penalty if the terms and conditions are varied during the service.

> **Recommendation 6:** The protocol should require signatories to undertake to honour the terms and conditions of a consumer contract for the duration of the contract.

Lastly, we note that it is problematic to frame this discussion in terms of 'barriers' to cloud uptake. Consumer concerns about privacy and security, for instance, may be preventing more consumers from adopting cloud services. By labelling such concerns as 'barriers', there is a real risk that the protocol will be directed towards removing these consumer concerns rather than towards reducing the risks and harms that are giving rise to these concerns. A reduction in consumer concern will follow from a reduction in these risks and harms, as well as through increased transparency from cloud providers.

> **Recommendation 7:** In developing the protocol, the focus should be on reducing consumer risks and harms rather than on overcoming 'barriers'.

2.4. Question 7. If a voluntary protocol is introduced, do you have any comments on potential compliance costs, jurisdictional complexities and the interaction between the Protocol and other cloud standards currently being developed globally?

As noted above, we are concerned about the addition of yet another voluntary code to the many voluntary codes and standards currently in existence that may apply to cloud services, such as the Telecommunications Consumer Protections Code,[8] ASIC's ePayments Code,[9] the Internet Industry Association's iCode,[10] Content Services Code[11] and Approved Vendor Trust Marque,[12] the New

[8] <http://commsalliance.com.au/Documents/all/codes/c628>
[9] <https://www.asic.gov.au/asic/asic.nsf/byheadline/ePayments-Code>
[10] <http://icode.net.au/>
[11] <http://iia.net.au/userfiles/content_services_code_registration_version_1_0.pdf>

Zealand CloudCode, the Cloud Industry Forum's Code of Practice,[13] various accreditations against ISO information security standards,[14] and for-profit accreditation schemes such as those offered by TRUSTe.[15]

The results of this plethora of voluntary codes and schemes are that (i) consumers are likely to be overwhelmed by the range of compliance arrangements that a provider claims to have met; (ii) providers are likely to be forced to pay for and sign up to multiple arrangements out of a fear of appearing to have substandard policies and practices; and (iii) consumers will have essentially no greater protection than they would have in the absence of the various codes and schemes, albeit that they might have the mistaken belief that the codes and schemes offer some protection. Providers may also find that the increase number of compliance considerations leads to increased costs or decreased service quality, which will have a negative impact on consumers.

2.5. Question 8. Using the New Zealand Code as an example, are there changes or improvements that could be made which would improve the efficacy of that process in an Australian context? Are there other issues not addressed in the New Zealand Code that need to be considered?

The New Zealand CloudCode has several shortcomings that, while perhaps a necessary result of it being a voluntary code, limit the consumer benefits of the CloudCode and the confidence that the CloudCode may give consumers about using cloud services.

2.5.1. Complaints and redress

While the CloudCode does set out a complaints process, the possible outcomes of that process are limited to:

- That no further action is required;
- That the signatory complained about must 'update a disclosure statement or correct an anomaly';
- A referral of the matter to a relevant authority;
- That the signatory be withdrawn from the Code register.

These outcomes provide little incentive for a signatory to comply with the CloudCode. The outcomes also provide little in the way of incentive for a consumer to make a complaint—the most a consumer can hope for from the time and effort needed to lodge a complaint is that the signatory will be asked to update their disclosure statements or lose the marketing value of being a signatory. If the protocol similarly provided no incentive to make a complaint, then any value in having a complaint process in a voluntary code would be undermined.

---

[12] <http://iia.net.au/iia-approved-vendor-trust-marque>
[13] <http://www.cloudindustryforum.org/>
[14] <http://www.27000.org/>
[15] <http://www.truste.com/>

Recommendation 8: The protocol must require signatories to participate in a complaints process that can deliver outcomes for consumers.

Useful complaint outcomes for consumers might include, for example, a direction for a provider to pay compensation, a direction for a provider to provide a specific service, a direction for a provider to carry out—or stop carrying out—an act, or a direction for a provider to amend a charge. While many of these outcomes may be attainable through other avenues (such as the Australian Consumer Law) a simple, central and low-cost avenue for complaints and dispute resolution would reduce both the risk and the perceived risk to consumers in using cloud services.

Signatories to the protocol must have internal dispute resolution (IDR) processes in place, and where a complaint is not resolved to the consumers' satisfaction by IDR the consumer should have recourse to an independent external dispute resolution (EDR) service, and this requirement should be set out in the protocol. Requirements for independent adjudicators exist, for instance, for privacy codes under s 18BB of the *Privacy Act 1988* and for financial sector codes under cl 183.25 of ASIC's code development guidelines. The existence of an independent dispute resolution process is an important element for ensuring that consumers have confidence in the protocol as an instrument of consumer protection rather than as a marketing device for industry. The CloudCode allows for a 'panel of independent experts' to be convened (cl 6.3) but the decision to convene such a panel, and the initial investigation of a complaint, rests with an undefined 'CloudCode investigation team'. This arrangement is unacceptable and should not be adopted in the proposed cloud protocol.

Recommendation 9: Dispute resolution should be attempted in the first instance by internal dispute resolution processes. An independent external dispute resolution service must be available for consumers who are not satisfied by the result of internal dispute resolution. Both dispute resolution mechanisms should be available at no cost to the consumer.

2.5.2. Compliance monitoring and enforcement

The CloudCode lacks any real compliance or enforcement mechanisms. The importance of enforceability and compliance monitoring has been noted in the code development guidelines issues by, for instance, the Office of the Australian Information Commissioner[16] and the Australian Securities and Investments Commission.[17]

As a voluntary instrument, the protocol will of course have limited enforceability. However, some simple steps would strengthen the protocol to some degree:

- Reports following a complaint process should be published, with the complainant's personal information removed. While exceptions may be appropriate for frivolous or vexatious complaints, the default position should be one of transparency.

[16] Office of the Australian Information Commissioner, *Code development guidelines*, September 2001, <http://www.oaic.gov.au/images/documents/migrated/migrated/cdg_01.pdf>.
[17] Australian Securities and Investments Commission, *Regulatory guide 183: approval of financial services sector codes of conduct*, 2005, <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/rg183-published-1-March-2013.pdf/$file/rg183-published-1-March-2013.pdf>.

- Signatories that are directed to update their policies following a complaints process should be clearly identified, along with the nature of the complaint and the details of the policy change.
- Signatories that are withdrawn from the register of signatories after a complaint should be clearly identified in a separate list, so that consumers are able to readily identify providers who have committed serious violations of the protocol.

Although an unenforceable protocol will provide limited additional consumer confidence in cloud services, transparent and independent processes directed towards making cloud providers accountable for their behaviour will help to ensure that the protocol is at least seen as encouraging some positive changes in providers' behaviour.

> **Recommendation 10:** The protocol should require that reports of the outcomes of complaint processes be published. Reports should be anonymised to protect the complainant.
> **Recommendation 11:** There should be clear identification of signatories that have been directed to update their policies or that have been withdrawn from the register as a result of a complaint.

In addition, there must be regular audits of signatories (or at least a significant sample of signatories) in order to identify any signatories who have failed to comply with the protocol. It is inadequate to wait for a consumer to detect and complain about a non-compliant provider.

> **Recommendation 12:** Regular audits should be conducted to ensure that signatories comply with the protocol, rather than waiting for a complaint. Results of these audits must be made publicly available.

2.5.3. Governing body

The CloudCode makes multiple references to the 'CloudCode team'. This suggests that governance of the CloudCode will be the responsibility of an informal group within the Institute of IT Professionals NZ (the body that operates the CloudCode). This is not a satisfactory governance arrangement.

The Australian protocol must clearly set out what the governance structure of the protocol will be. In particular, the protocol must establish a protocol governing body and set out:

- The composition of the governing body;
- The process by which members of the governing body are chosen;
- The process by which members of the governing body are dismissed; and
- The powers of the governing body.

For individual and small business consumers to have any confidence in the protocol, it is important that their interests are represented—and perceived as being represented—in the governing body. The protocol should therefore require that at least one (but ideally more than one) position on the governing body is occupied by a consumer representative.

Recommendation 13: The protocol should specify the nature, powers and composition of a governing body responsible for managing the protocol.
Recommendation 14: The governing body should include at least one consumer representative.

2.5.4. Misuse of trustmarks

The CloudCode is largely based around the right of a signatory to use the CloudCode logo when promoting their products and services in order to gain user trust. This 'trustmark model' has been used for a number of years in the e-commerce, and is held to be a way to demonstrate to consumers that a particular provider complies with best practice—if the consumer sees the logo, they can put their concerns to rest.

In reality, the trustmark model is deeply flawed.[18] The core problems with the trustmark model include:

- It may be difficult to establish consumer recognition of and confidence in the trustmark. While some trustmarks associated with well-known brands may be recognised, it may be difficult to establish a new trustmark from scratch. It may also be difficult to encourage confidence in that trustmark—why should a consumer feel safer because a website uses a well-designed image?
- There are multiple trustmarks in the market, and consumers may find themselves overwhelmed by the number of marks that appear on a webpage or advertisment.
- There is a real risk of 'false confidence' being created. Since there is no restriction on who can create a trustmark or what standards a trustmark must meet, there is no good reason for consumers to have confidence in a particular trustmark, except to the extent that they have confidence in the organisation that establishes the trustmark.
- Trustmarks are often provided to companies for a fee (whether the fee is for the trustmark itself or for membership in an organisation), and the concern that a trustmark may be influenced by business interests rather than concerns for consumer protection may negatively impact the trustmark.
- There are generally no technical measures to prevent a non-signatory from using the trustmark—it is a simple matter for any organisation to include the image on their website. The possibility of an unauthorised company presenting itself as a signatory places consumers at risk and undermines confidence in the trustmark. In the cloud services context, any sense that the market is being overrun by untrustworthy vendors is likely to undermine confidence in cloud services and reduce uptake.

If the protocol is to make use of a trustmark model similar to that in the CloudCode, then several important elements must be included in the protocol:

- The protocol's governing body must establish a public list of signatories on its website—the CloudCode includes such a provision.
- The public register must be regularly maintained to ensure that all signatories remain compliant with the protocol. A signatory should automatically be removed if a decision to

[18] Connolly C, *Trustmarks struggle to protect privacy*, 2008, <http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf>.

that effect is made following a complaint of if the signatory fails to pay any fees or otherwise maintain their signatory status.
- The protocol governing body must undertake to act against any business that uses the trustmark without being a signatory to the protocol. At a minimum, when any such business is identified it should be included on a public list, available alongside the list of signatories on the governing body's website.

> **Recommendation 15:** A list of signatories to the protocol must be maintained on a public website.
> **Recommendation 16:** The list of signatories must be maintained to ensure that the information is up to date.
> **Recommendation 17:** Cloud providers that falsely claim to be signatories must be clearly identified in a public list.

2.5.5. Regular and open reporting

As suggested above, transparency will be an important element of ensuring that a voluntary protocol can improve consumer confidence in cloud services. As well as reporting on the outcomes of complaints, the protocol's governing body should publish regular and open reports on the operation of the protocol, addressing at least the following points:

- The total number of signatories to the protocol;
- The number of complaints made about signatories;
- The nature of complaints made, including the general nature of those complaints (e.g. whether the complaint relates to privacy, reliability, interoperability, etc.);
- The outcomes of those complaints; and
- Any systemic issues identified by the governing body.

> **Recommendation 18:** There should be regular and open reporting of the operation of the protocol.

2.5.6. Review of the protocol

As in the CloudCode, there should be a requirement in the protocol for a regular review of the protocol. The need for such a review highlights the need for regular reporting as outlined above. However, where the CloudCode requires only the 'support of the Cloud Computing industry', the protocol reviews should require the support of industry and other stakeholders, and in particular consumer representatives. Consumer representatives should be directly informed of reviews by the protocol's governing body to ensure that the reviews reflect a range of interests, and not just the interests of cloud providers.

> **Recommendation 19:** Regular reviews of the protocol should be conducted, with a range of stakeholders consulted.