ADR Bulletin
ADR Bulletin

Volume 7 | Number 1 Article 1

6-1-2004

The issue of security in ODR

Camille Pecnard

Recommended Citation
Pecnard, Camille (2004) "The issue of security in ODR," *ADR Bulletin*: Vol. 7: No. 1, Article 1.
Available at: http://epublications.bond.edu.au/adr/vol7/iss1/1

This Article is brought to you by ePublications@bond. It has been accepted for inclusion in ADR Bulletin by an authorized administrator of ePublications@bond. For more information, please contact Bond University's Repository Coordinator.

ADR bulletin
The monthly newsletter on dispute resolution

Information contained in this newsletter is current as at June 2004

Volume 7 Number 1

Online dispute resolution

The issue of security in ODR

Camille Pecnard

General Editor

Laurence Boulle
Professor of Law,
Bond University, Queensland

contents

1
The issue of security in ODR

6
Nothing new in ADR

7
Doing it better — behaviour indicia of superior negotiators Part 2

10
The stamp of statistical approval

12
Mediating in the family business

20
Diary and happenings

Introduction

Security is a key issue in ODR, as it is in e-commerce in general, since it concerns the reliability of technology for users.

Terminology and definitions of 'security' fluctuate in the literature. Indeed, there seems to be no precise definition of security, combining as it does many different aspects, such as 'confidentiality',[1] 'secrecy',[2] 'transparency',[3] 'authentication, signature',[4] 'integrity',[5] 'control of information'[6] and 'privacy'.[7] Despite the breadth of the concepts encompassed by the term 'security', the main focus of security in ODR is protecting information.

> Protecting information has two aspects: the transmission and the storage of information … [which] are exposed to identical risks: unauthorised third parties must not be capable of accessing the information … and, *a fortiori*, altering this information … .[8]

Security is essential for creating trust and confidence in the online environment. Trust is identified by David R Wilkinson[9] as the 'third significant factor critical to the development of the e-society' in addition to 'awareness' and 'access'. Moreover, Katsh and Rifkin 'believe, frankly that trust is as important for the success of any web-based enterprise as convenience, but [they] also recognise that it is easily ignored and neglected.'[10]

On the one hand, security fosters trust in the technology used in the ODR process. On the other hand, a secured ODR system is one of 'the elements that are nowadays under consideration for augmenting the consumers' confidence'[11] in the online environment.

Although security builds trust in ODR, it is important to note 'that no communication method [even in an off-line environment] can provide absolute security.'[12] Traditional or 'snail' mail, facsimiles and e-mails can all potentially be intercepted, although civil and criminal protections exist in most countries to protect the security and secrecy of correspondence from unauthorised access by third parties.

New technology creates new issues, requiring new and more appropriate solutions. The internet and its associated technologies 'have not been developed with security, dependability and trust in mind,'[13] and 'it is often assumed that trust is a factor that cannot really be controlled.'[14] Despite the fact that 'the internet is not inherently trustworthy',[15] it is not impossible to significantly improve its security. '[S]ecurity is always a question of risk management, requiring a careful assessment of risks and balancing of risk with costs of implementing security.'[16] In relation to ODR processes, the security measures needed will depend on the specific needs of specific situations.

In this article I discuss the need for confidentiality in ODR, before looking at the technological tools available to protect the transmission of communications. I conclude by examining the issues of confidentiality and privacy in relation to the storage of information.

ADR Bulletin

Editorial Panel

Nadja Alexander
Professor of Dispute Resolution, Director of Practice Australian Centre for Peace and Conflict Studies, University of Queensland

Tom Altobelli
Associate Professor, School of Law, University of Western Sydney

David Bryson
Conciliation Officer, WorkCover Conciliation Service, Victoria

Peter Condliffe
Barrister, Specialist Mediator and Facilitator, Victoria

Margaret Halsmith
Consultant, Mediator, Facilitator, Trainer, Perth

Shirli Kirschner
Resolve Advisors Pty Ltd, Sydney

Michael Mills
Partner, Freehills, Sydney

Confidentiality in ODR

The issue of confidentiality in dispute resolution

Confidentiality as an issue in dispute resolution generally is complex and varies according to different situations and the different types of information exchanged between parties.

Parties may be very concerned to ensure that proceedings are not disclosed to the public because 'a dispute resolution process can be expected to produce more satisfactory results when each party is assured that the information gathered during the proceeding will not be further communicated, unless permission is given to do so.'[17] The goal of non-disclosure is therefore to protect parties' reputations and to establish an environment of trust and confidence between them.

For some types of information exchanged between the parties there is protection against unauthorised third parties. Other types of information exchanged between one of the parties and the mediator/arbitrator may be protected by nondisclosure to the other party.

Proceedings may not always be required to be confidential. In certain circumstances the law may require disclosure of information, while in others the publication of proceedings may be required in order to provide transparency. This disclosure may be justified as protecting consumers and providing 'legal certainty.'[18] Indeed, 'consumer associations often stress the point that a possibility to "name and shame" untrustworthy marketplaces should be provided by dispute resolvers.'[19]

The need for confidentiality in ODR

The 'confidentiality' or 'secrecy' of information is very important for the security of ODR. The need for confidentiality in ODR will differ according to whether the dispute involves a negotiation, mediation or arbitration. In an automated negotiation or blind bidding, 'the offers and demands expressed by the parties are not revealed to any individual, not to the other party nor to any other person.'[20] In assisted negotiation or mediation, parties are likely to expect total confidentiality as it concerns no one but them.

ODR institutions generally have a policy regarding the confidentiality of information. For example, the SmartSettle facilitation and mediation agreement states that 'all information disclosed to the facilitator … is confidential unless within the public domain' and 'the facilitator shall not, nor shall the facilitator authorise anyone else, directly or indirectly, during the negotiation process or afterwards, divulge any Confidential Information to any person or other party to the negotiation process without the express authority of the party disclosing the Confidential Information.'[21]

In ODR, as in ADR generally, there is a trend towards transparency, with a certain amount of information able to be disclosed. For example, 'information related to the proceedings is sometimes publicised as aggregate data (without revealing the identity of the parties or enabling a dispute to be identified).'[22] According to Orna Rabinovitch-Einy, 'it seems likely that most, if not all, agreements will be made public, while the mediation sessions themselves will remain confidential.'[23] In certain circumstances, total disclosure can also be required.

> One online arbitration service, WIPO (World Intellectual Property Organisation) has already, for example, adopted a policy of transparency and has mandated the publication of resolutions on its website [with the names of parties], which is accessible to all internet users.[24]

In addition to establishing adequate rules to protect information in ODR from being disclosed to unauthorised parties, some technological tools can be implemented to protect the transmission of such information.

Technological tools protecting the transmission of communications in ODR

Transmission of communications

Parties in the course of ODR proceedings will necessarily exchange a lot of information, such as discussions regarding the issue, proofs of their different arguments, and agreements or settlements resulting from the

negotiation or mediation. Information may be transmitted to other parties via many different technological means, such as emails, chat rooms, discussion boards or videoconferencing, which, as we have seen, were not created with 'security and trust in mind.'[25] The ODR provider's confidentiality of information statement 'does not necessarily imply that such information cannot be transmitted or accessed accidentally or that it cannot be accessed by third parties.'[26] Indeed, it is often said that standard email is no more secure than a postcard.[27]

Parties first need to be sure that messages communicated between them remain confidential and safe from prying eyes. Next, parties will generally require that the integrity of transmitted documents is guaranteed (ie that they have not been subject to tampering). Finally, parties need to be assured that the message is from the right person. The goal is to avoid, as often as possible, repudiation from the other party.

Information may be transmitted to other parties via many different technological means, such as emails, chat rooms, discussion boards or videoconferencing, which, as we have seen, were not created with 'security and trust in mind.'

Technological tools

Many different tools have been developed to achieve the confidentiality described above. 'Username and passwords, digital signatures and encrypted messages are most commonly used,'[28] bearing in mind that '[the] level of security [that] is appropriate for a particular mediation will depend on the dispute and the requirements of the parties.'[29]

In addition to usernames and passwords, which limit access to email addresses, chat rooms or internet discussion boards to authorised and identified parties, the 'risk of repudiation and alteration of a message can also be reduced by digital signatures.' Using symmetric or private keys systems, where the same key encrypts and decrypts the message, or asymmetric or public keys systems, where two different but related keys are needed to encrypt and decrypt, 'the receiver of an electronically signed message can verify the origin, the integrity of the message'[30] and the identity of the sender.

Based on symmetric and asymmetric systems, different encryption options, such as the Secure Multipurpose Internet Mail Exchange Protocol (S/MIME) or Pretty Good Privacy (PGP) may be implemented to protect emails. With S/MIME protocol, 'it is possible to authenticate the origin of the email and to ensure the confidentiality and integrity of its content'.[31] PGP 'provides the same quality of service as S/MIME.'[32]

Other tools protect web-based communication and 'allow parties to communicate on a secure web page or platform.'[33] The most frequent and common method is the Secure Sockets Layer (SSL), 'indicated by a website beginning with "https" [instead of the traditional "http"] or a lock symbol on the user's screen.'[34] SSL-secured HTTP protects the confidentiality and integrity of the data transmitted.

To avoid the 'risk of virus infections, intrusions or disk crashes … firewalls, backup policies and intrusion detection systems are the standard mechanisms.'[35] Finally, biometrics, like fingerprint, retinal, voice-print or genetic patterns, may involve many possibilities to improve online security in the future.

Limits of technological protection

As we have seen, there are many different technological protections which have been developed to protect and secure online communications in ODR. However, with respect to email, for example, 'they are not in general use. The current estimate is that only 0.5% of email is encrypted in any way (Rule 2002:246).'[36] Some authors say that, in spite of its convenience and its potential to be secure, 'email is not the main communication method used by modern online ADR systems'[37] and web-based communications are preferred.

There are certain risks inherent in the technological protections described. Whatever the security tools used, the inherent complexity of technology can create diverse problems that can affect the transmission of communications between the parties. ODR providers, like SmartSettle in its Facilitation and Mediation Agreement para 8, may establish that 'the parties acknowledge that, due to the inherent complexity of computer programs and mathematical models, the System may not be completely free of errors. The parties agree not to base any decisions solely on results that may be generated by the System or suggestions of the Facilitator(s) without verification.'[38]

In addition, as technology evolves every day, certain old encryption standards, like the Data Encryption Standard (DES) developed in 1977 by IBM, have become obsolete considering that they are easy to break these days. Similarly, security tools that are effective at the moment may well become out of date in the near future.

Finally, an important risk involves the human element. Even though the means of transmitting information may be secured, the intervention of a third party at sending and receiving computers, described by Richard Hill as 'the real weak points',[39] is still possible. 'The point is that the real risk to confidentiality comes from within an organisation's office, not from somebody tapping into communications infrastructure somewhere in the middle of the ocean.'[40] Indeed, access to information may occur in many cases where the disclosure of usernames and passwords are directly or accidentally provided to someone else, 'for example by reading the post-it under the keyboard or in a desk drawer.'[41]

Protection of stored information

The storage of information

In ODR processes, whatever means are used, there is automatic storage of all information exchanged by the parties. This is recognised by mediators/arbitrators and many authors as 'one of the significant benefits of ODR … for building feedback and intelligence into the ODR process … [and] in recreating who said what, what was said, and under what circumstances.'[42] Indeed, in comparison to the off-line environment, where, particularly in face-to-face meetings, most of the discussion is oral, the transcript of exchanges between parties allow the third party to review the course of the discussion in order to provide a more efficient intervention.

However, this automatic storage of information can create privacy problems in relation to personal information. Parties need to have control of their own information, to determine who can gain access to information and on what terms. In the course of ODR proceedings, parties may reveal sensitive personal information that needs to be protected and only disclosed to others with their consent.

Technical solutions

There are technical tools used by ODR providers to protect the privacy of stored information. Storage site systems can be protected by firewalls (which thus also protect individual records) and encryption, which also ensures the protection of personal information. Other new technologies 'may enhance privacy in a digital age,'[43] such as intelligent agents like Platform for Privacy Preferences (P3P),[44] which can 'automatically negotiate a privacy agreement between parties to a transaction before a deal is done.'[45] Some organisations, such as TRUSTe,[46] also 'provide a trust mark to those internet sites and businesses that adhere to a set of privacy principles and dispute resolution procedures.'[47]

Legal protection

The use and disclosure of personal data is, to some extent, protected around the world. Under Australian law, for example, the monitoring of discussions requires the consent of the other person. The National Privacy Principles deal with the collection of personal information, its use and disclosure. The *Privacy Amendment (Private Sector) Act* 2000 (Cth) gives 'organisations and industry an opportunity to develop their own codes of conduct regarding privacy.'[48] Therefore, 'it is critical that an online dispute resolver explicitly state how information provided by the parties will be used.' The SmartSettle agreement establishes, for example, that 'after the completion of the negotiation process, the Facilitator will, at the written request and expense of the parties, destroy all or any Confidential Information to which s/he has access, whether in hard form or resident in any computer storage media ….'[49] 'Others (ODR providers) can store it in case of the disputant losing their own data (Intersettle).'[50]

Conclusion

As we have seen, the issue of security principally concerns the confidentiality of information, the transmission of communication and the protection of stored data. ODR providers need to satisfy certain security requirements addressing these concerns in order to improve the trustworthiness of their service. They also need to implement adequate technological security tools and respect explicit privacy policies. There are 'best practice principles on security and privacy that should be built into any online ADR system developed',[51] which can be sourced through various proposed guidelines for best practice elaborated by, for example, the American Bar Association (ABA),[52] the National Alternative Dispute Resolution Advisory Council (NADRAC)[53] and the Department of Justice in Victoria.[54]

Security is one of the most important elements for the continuing development of ODR. However, its importance will probably diminish in the coming years with the development and general application of advanced technologies and the increasing trust internet users have in their online environment. ●

Bibliography

American Bar Association (ABA), Proposed guidelines for recommended best practices by ODR service providers, Report, 2002.

Bills K, *Are you using Online Dispute Resolution*? September, 2002.

Conley Tyler M, Bretherton D, *Seventy-six and Counting: An analysis of ODR sites*, Proceedings of the UNECE Forum on ODR 2003, <www.odr.info/unece2003>, accessed 11 April 2004.

Conley Tyler M, Bretherton D, Firth L, *Research into online Alternative Dispute resolution*, Feasibility report prepared for the Department of Justice, Victoria, 20 June 2003.

Forder J, Quirk P, *Electronic commerce and the law*, Wiley, 2nd ed, 2003.

Hill R, *E-government and ODR*, Proceedings of the UNECE Forum on ODR 2003, <www.odr.info/unece2003/pdf/Hill.pdf>, accessed 11 April 2004.

Hornle J, 'Online Dispute Resolution: The Emperor's New Clothes?' *International Review of Law Computers and Technology*, Vol 17 No 1, pp 27-37, 2003.

Katsh E, Rifkin J, *Online Dispute Resolution*, Jossey Bass, 2001.

National Alternative Dispute Resolution Advisory Council (NADRAC), *Dispute Resolution and Information Technology Principles for Good Practice*, March 2002.

P3P: <www.w3.org/P3P>.

Rabinovich-Einy O, 'Going public: Diminishing Privacy in Dispute Resolution in the Internet Age', Summer 2002, 7 Va JL and Tech 4, <www.vjolt.net/vol7/issue2/v7i2_a04-Rabinovich-Einy.pdf>, accessed 11 April 2004.

Schultz T, Bonnet V, Boudaoud K, Kaufmann-Kohler G, Harms J, and Langer D, *Electronic Communication Issues Related to Online Dispute Resolution Systems*, Proceedings WWW2002 of The Eleventh International World Wide Web Conference – Alternate Track CFP: Web Engineering, Honolulu, Hawaii, Conference on 7-11 May 2002, <www2002.org/CDROM/alternate/676/>, accessed 11 April 2004.

SmartSettle, Smartsettle Facilitation and Mediation Agreement, <www.smartsettle.com/family/content.php?facilitationagreement.html>, accessed 17 March 2004.

TRUSTe: <www.truste.org>.

Wilkinson D R, *Protection and Security of Citizens in the Information Society*, Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission, <www.itas.fzk.de/e-society/preprints/vulnerability/Wilkinson.pdf>, accessed 11 April 2004.

Camille Pecnard has a law degree in France and a Master of Laws (LLM) specialising in Intellectual Property, Information Technology and E-commerce at Bond University, Queensland, Australia. He can be contacted at <camillepecnard@hotmail.com>.

Endnotes

1. Hill R, *E-government and ODR*, Proceedings of the UNECE Forum on ODR 2003, <www.odr.info/unece2003/pdf/Hill.pdf>, accessed 11 April 2004.
2. Rabinovich-Einy O, *Going public: Diminishing Privacy in Dispute Resolution in the Internet Age*, Summer 2002, 7 Va JL & Tech 4, <www.vjolt.net/vol7/issue2/v7i2_a04-Rabinovitch-Einy.pdf>, accessed 11April 2004.
3. Above note 2.
4. Above note 1.
5. Forder J, Quirk P, *Electronic commerce and the law*, Wiley, 2nd ed, 2003.
6. Above note 2.
7. Above note 2.
8. Schultz T, Bonnet V, Boudaoud K, Kaufmann-Kohler G, Harms J, and Langer D, *Electronic Communication Issues Related to Online Dispute Resolution Systems*, Proceedings of WWW2002 – The Eleventh International World Wide Web Conference – Alternate Track CFP: Web Engineering, Honolulu, Hawaii, conference on 7-11 May 2002, <www2002.org/CDROM/alternate/676/>, accessed 11April 2004.
9. Wilkinson D R, *Protection and Security of Citizens in the Information Society*, Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission, <www.itas.fzk.de/e-society/preprints/vulnerability/Wilkinson.pdf>, accessed 11April 2004.
10. Katsh E, Rifkin J, *Online Dispute Resolution*, Jossey Bass, 2001, p 83.
11. Above note 9.
12. Hornle J, 'Online Dispute Resolution: The Emperor's New Clothes?' *International Review of Law Computers & Technology*, Vol 17 No 1, pp 27-37, 2003.
13. Above note 9.
14. Above note 9, p 85.
15. Above note 9, p 85.
16. Conley Tyler M, Bretherton D, *Seventy-six and Counting: An analysis of ODR sites*, Proceedings of the UNECE Forum on ODR 2003, <www.odr.info/unece2003>, accessed 11 April 2004.
17. Above note 8.
18. Above note 8.
19. Above note 8.
20. Above note 8.
21. SmartSettle, *Smartsettle Facilitation and Mediation Agreement*, <www.smartsettle.com/family/content.php?facilitationagreement.html>, accessed 17 March 2004.
22. Above note 8.
23. Above note 2 at 37.
24. Above note 8 at 38.
25. Above note 9.
26. Above note 8.
27. Above notes 8 and 16.
28. Bills K, *Are you using Online Dispute Resolution?* September 2002.
29. Above note 28.
30. Above note 8.
31. Above note 8.
32. Above note 8.
33. Above note 16.
34. Above note 16.
35. Above note 16.
36. Above note 16.
37. Above note 16.
38. Above note 21.
39. Above note 1.
40. Above note 1.
41. Above note 1.
42. Above note 10.
43. Above note 5.
44. P3P: <www.w3.org/P3P>.
45. Above note 5.
46. TRUSTe: <www.truste.org>.
47. Above note 5.
48. Above note 5.
49. Above note 21.
50. Above note 16.
51. Conley Tyler M, Bretherton D, Firth L, *Research into online alternative dispute resolution*, Feasibility report prepared for the Department of Justice, Victoria, 20 June 2003.
52. American Bar Association (ABA), *Proposed guidelines for recommended best practices by ODR service providers*, Report, 2002.
53. National Alternative Dispute Resolution Advisory Council (NADRAC), *Dispute Resolution and Information Technology Principles for Good Practice*, March 2002.
54. Above note 51.