ELECTRONIC COMMUNICATION ISSUES RELATED TO ONLINE DISPUTE RESOLUTION SYSTEMS

T. SCHULTZ, V. BONNET, K. BOUDAOUD, G. KAUFMANN-KOHLER, J. HARMS, and D. LANGER, "Electronic Communication Issues Related To Online Dispute Resolution Systems", Proc. WWW2002 – The Eleventh International World Wide Web Conference – Alternate Track CFP: Web Engineering, Honolulu, Hawaii, conference on 7-11 May, 2002, <http://www2002.org/globaltrack.html>

V. Bonnet, K. Boudaoud, J. Harms
Centre Universitaire Informatique
University of Geneva, Switzerland
Phone: (41) 22 705 76 35
E-mail: {Vincent.Bonnet, Karima.Boudaoud, Juergen.Harms}@cui.unige.ch

T. Schultz, G. Kaufmann-Kohler, D. Langer
Faculty of Law,
University of Geneva, Switzerland
Phone: (41)22 705 85 03
E-mail: {Thomas.Schultz, Gabrielle.Kaufmann-Kohler, Dirk.Langer}@droit.unige.ch

Abstract

The rapid growth of electronic commerce increases the potential for conflicts over contracts which have been entered into online (e.g. about price, late delivery, defects, specifications ...). Thus, the use of online dispute resolution (ODR) mechanisms to resolve such e-commerce conflicts is crucial for building consumer confidence and permitting access to justice in an online business environment. However, the use of the Internet and the World Wide Web in dispute resolution has an impact on the types of communication implied in the relevant processes (negotiation, mediation and arbitration), and involves new security issues such as the integrity and confidentiality of sensible data and communication mechanisms used to transmit and store this data. This paper deals with electronic communication issues with respect to the ODR processes.

Keywords: online dispute resolution, law, dispute resolution processes, electronic commerce, World Wide Web, electronic communication, security, interdisciplinary.

Introduction

The number of businesses and customers transacting over the Internet is increasing rapidly and transactions generate disputes, for instance about price, quality, time of delivery [1]. In fact, dispute on the World Wide Web is growing as rapidly as e-commerce itself [2]. According to DataQuest Research, the total value of e-commerce transactions around the world will reach US $1 trillion in 2003, with each transaction potentially triggering a dispute [2]. Therefore, the future growth of e-commerce depends on providing consumers and businesses with greater confidence, which in turn necessitates a possibility to access justice and a predictable outcome of

disputes arising in the online environment. One solution to handle such disputes related to e-commerce is to use, rather than traditional court litigation, alternative online dispute resolution (ODR) mechanisms. Resolving disputes over the Internet is likely to play an important role in the future of electronic commerce.

The field of dispute resolution can in fact not avoid being affected by the new information technologies because communication is central to this process [5]. Actually, the integration of the Internet and the World Wide Web in dispute resolution has an important impact on communication types involved in the relevant processes. For instance:

1. parties to a dispute may use the Internet to communicate with one another as part of a negotiation process [5];

2. a neutral party might communicate with both parties via the Internet as part of a mediation or arbitration [5].

Moreover, a large number of dispute resolvers have Web sites where they describe and promote their services. They also use emails to communicate with their clients and colleagues and send "attached" files with emails [6].

Globally, in addition to facilitating communications between parties involved in a dispute, the Internet and the World Wide Web may facilitate the collection, transmission and storage of information pertaining to the dispute. However, despite the obvious advantages of electronic data support and communication procedures, they show drawbacks, particularly in terms of security. In this paper, we discuss the electronic communication issues

1. involved in ODR processes, and

2. concerning protection of data used in these processes and electronic communication support used for transmitting and storing this data.

We also outline some other technical requirements such as adaptability and accessibility that seem important for ODR providers. The state of the art presented in this paper is a part of an interdisciplinary research project, named **e-Law**[3], which is conducted by the *Private International Law Department* of the University of Geneva and the *Centre universitaire informatique* of the Faculty of Science of the same university. This project aims at evaluating both legally and technologically the first experiments in online dispute resolution and to formulate, on this basis, recommendations for the improvement of dispute settlement mechanisms using information technology [3].

Our paper is organized as follows. First, we discuss the interactions between methods of communication, quality of justice, confidentiality and publication of results in the different ODR processes. Then, we deal with the security requirements for ensuring protection of electronic communication and data. Thereafter, we outline other technical properties that are also essential for ODR systems. Finally we conclude by giving general recommendations to ODR providers and discuss some areas for future work.

Related works

The term ODR generally means the electronic form of Alternative Dispute Resolution [3], although it is sometimes extended to include the simple use of the Internet and other web- and computer-based technologies for facilitating alternative dispute resolution [4]. Although there is a very large variety of existing ODR mechanisms, they can be classified in the same categories as those used for offline alternative dispute resolution [3][4][7]. First, there is negotiation, which

can be automated, in the sense that both parties try to come to an agreement by a 'blind-bidding' procedure. In such a procedure, each party successively offers an amount of money, which is not communicated to the other party. A computer compares the amounts and reaches a settlement for the parties if the figures are within a given spread [8]. The other form of negotiation is assisted negotiation, in which case the parties try to come to an agreement by actively communicating with one another over the Internet, using for instance emails, teleconferences or videoconferences. The main common feature of these two forms of negotiation is that no third human intervenes in the process. Second, there is mediation, a process in which a neutral person, called the mediator, communicates with both parties and tries to bring them to an agreement. Third, there is arbitration, a process in which a third party chosen by the parties, decides the case for them, after having heard the relevant arguments and seen the appropriate evidence [9][10].

There are many institutions that currently offer online dispute resolution services. However, as their business model is often confronted with conflicts of interests because of the need of independent financing, the field of ODR is still unstable. Current examples are the following:

- The institutions offering automated negotiation include: 1-2-3 Settle.Com [11], AllSettle.Com [12], ClickNsettle.com [13], Cybersettle [14], Intersettle [15], MARS [16], NewCourtCity [17], ResolveItNow.com [18], SettlementOnline [19], SettleOnline [20], SettleSmart [21], The Claim Room [22], U.S. Settle [23], WebMediate [24], and WeCanSettle [25].

- The institutions offering assisted negotiation include: ClaimChoice.com [26], ECODIR [27], iLevel [28], Online Resolution [29], the Resolution Forum [30], SquareTrade [31], The Claim Room [22], TRUSTe [32], and Web Trader [33].

- The institutions offering mediation include: 1-2-3 Settle.Com [11], Cybercourt (planned) [34], e-Mediator [35], ECODIR [27], eResolution [36], IntelliCOURT [37], Internet Neutral [38], MARS [16], ODR.NL (planned) [39], Online Resolution [29], Online Ombuds Office [40], NewCourtCity [17], OnlineDisputes (planned) [41], NovaForum.com [42], the Resolution Forum [30], SettleTheCase [43], SquareTrade [31], WebAssured.com [44], Web Dispute Resolutions [45], WEBDispute.com (planned) [46], WebMediate [24].

- The institutions offering arbitration include: 1-2-3 Settle.Com [11], Cybercourt (planned) [34], eResolution [36], IntelliCOURT [37], MARS [16], NovaForum.com [42], ODR.NL (planned) [39], Online Resolution [29], the Resolution Forum [30], SettleTheCase [43], SquareTrade [31], the Virtual Magistrate [47], WebAssured.com [44], Web Dispute Resolutions [45], WEBDispute.com [46], WebMediate [24] and Word&Bond [48].

These dispute resolution institutions apply different procedures, and use different kinds of electronic communication means. After having surveyed this variety of approaches to similar electronic communication issues, we have tried to present these issues consistently in order to seek uniform answers.

ODR and communication from law and justice point of view

Justice requires appropriate communication means

Solving dispute requires communication. Be it in court litigation or other forms of dispute resolution, the existence of rights and obligations has to be expressed, arguments have to be uttered, and reality has to be described to apply a fair process. The right and the capacity of the parties to communicate with the deciding body and the other party is an issue of due process, or

at least of quality of justice. Offline, due process and quality of justice often depend on questions of time: there has, for instance, to be a proper time-period for evidence and argumentation and the global length of the procedure has to be neither too short nor too long.

On the Internet, the importance of time is a little different, as for instance one of the characteristics of cyberspace is the worship of speed. Online dispute resolution follows the same trend and everybody argues that it has to operate very quickly. As a result, online proceedings are often short or even very short. This is usually considered legally acceptable, but only if the parties have had an appropriate possibility to communicate. An issue that is therefore often debated, with respect to ODR, is which are the proper means for evidence and argumentation? For instance, would simple email exchanges be enough? The answer to this question is different depending on the type of dispute resolution.

Communication tools currently used

In negotiation and mediation, communication is an important issue for the quality of justice they produce, as both these processes are psychologically based on communication. Of course, if the parties to a dispute resolution procedure decide that exchanging blind bids is enough communication, there is nothing legally objectionable about it. However, more sophisticated means of communication may lead to more subtle and more satisfying results. It is for instance widely acknowledged that the work of a mediator is essentially based on language [49]. Communication is full of subtleties and these subtleties can possibly predetermine the possibility of a settlement, be it in mediation or in negotiation, for instance by switching the atmosphere from war-like to journey-like. The parties often go into mediation being shut away in their entrenchment: the defendant, for instance, is often hard to bring to talk about quantum, since he is not liable and quantum is consequently not relevant [50]. The mediator therefore has to get the parties off their 'perches' and towards negotiating. For this purpose he must first understand what the parties want, which is not always money, and then he must build up trust between himself and the parties and between the parties themselves. This activity relies widely on atmosphere and communication nuances. For this purpose, it is often fundamental to observe body language and inflections in tone and voice, because they provide indications on the degree of trust, the willingness to reach an agreement, and the parties' genuine concerns and interests. To be best interpreted, these indications have to be related to the cultural and ethnic background, as well as to such factors as age and gender [51].

In terms of electronic communication means, the consequences are not so easy to draw. On the one hand, it has been shown that persons with good typing skills and a high data flow connection can easily dominate chat-room meetings [52]. This observations would advocate for real-time communication tools, preferably videoconferencing or teleconferencing. On the other hand, it has also been shown that typing and the resulting time lag caused persons to pay more attention to the substantive content of messages, lessened the emotional stress brought up by conflict resolution and made it easier to overcome socioeconomic differences [53]. This observations would advocate for sequential, broken up and relatively slow communication, such as emails

The survey of existing ODR mechanisms shows that assisted negotiation is almost always conducted only by emails, while mediation procedures show more variations. Although the range of available communication means in a given online mediation procedure is often unclear or flexible, some rules restrict the communications to emails while others allow a large variety of means, which covers emails; telephone calls or teleconferencing; web-based real-time conferencing or message posting; videoconferencing; fax; voice mail; and even postal mail and hand delivery.

In arbitration, the availability of appropriate communication means implicates even more than

the quality of justice. If the relevant evidence and arguments cannot be adduced by appropriate means, the process runs the risk of violating due process [54]. In this case, the arbitration may simply be set aside by a court, or the entire procedure may be denied the qualification of arbitration, which signifies that the decision is much more difficult to enforce, as valid arbitration awards are binding on the parties like a judgment [55].

The categories of communication tools available in arbitration are almost the same as in mediation, that is emails; telephone calls or teleconferencing; web-based communication; videoconferencing; fax; and, for arbitration, in-person hearings.

Publication vs. Confidentiality

The publication of ODR proceedings is a controversial issue. On the one hand, 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 [56]. On the other hand, the publication of these results provides transparency, it helps the parties to have a clearer expectation about the proceedings and their possible outcomes. Consumer associations often stress the point that a possibility to 'name and shame' untrustworthy marketplaces should be provided by dispute resolvers. In this sense, the publication of case results is an issue of legal certainty. Globally, the controversy is almost solved when turning to the distinction between business-to-business and business-to-consumer relationships. In the first case, the parties often seek anonymity and the preferred solution is not to publicize the results. In the second case, the consumer often needs or deserves the protection of publicity.

In any case, the publication of results certainly aims only at certain types of documents, and at a specific time. This means that there always has to be some confidentiality (which in legal terms means that a given information *has*to remain unaccessible to third parties, not that it is actually secured).

Offline ADR takes place in physical spaces, and the parties can therefore, from the context alone, assume that sensible information is not communicated to third persons, but this is not the case online. Documents are copied more often and deletion can hardly be proven [56]. Therefore, ODR institutions should at least provide clear provisions on confidentiality.

Current policies concerning publication and confidentiality

In automated negotiation, all institutions except one operate on the basis of 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. The submitted figures are usually deemed (they will not be revealed to anybody), no matter if the case settles or not. Only one provider reserves the right to publish outcomes in the future, and another provides general bidding statistics.

In assisted negotiation, the institutions usually have a privacy policy stating that all information gathered during the proceedings is kept confidential. However, some institutions publicize the claim if a B2C dispute does not settle, or the result, if a trustmark has been revoked because of infringements by the merchant.

In mediation, the importance of confidentiality is often stressed, as there is an intrinsic need for this: in order to achieve satisfactory results, mediation has to take place in a context in which the parties and attorneys can communicate openly, without fear that these statements may be used against them outside the mediation. The possibility to discuss facts and issues openly is necessary to come to solutions and settlements [50]. In online mediation, all institutions hold

private and confidential the proceedings proper. Case results are never published as such. However, information related to the proceedings are sometimes publicized as aggregate data (without revealing the identity of the parties or enabling a dispute to be identified). However, one mediation provider specifies that the documents provided by the parties are only legally privileged until the settlement of the dispute.

In arbitration, the parties usually expect confidentiality, although there is no general obligation of confidentiality in international arbitration [57]. The survey of existing policies reveals that the privacy of the proceedings proper is almost always provided (outsiders are practically never allowed to attend the hearings, nor do they have a right of access to the record of the proceedings). Prior to the proceedings, no information is publicized and no list of pending arbitrations can be investigated. After the proceedings, a very large majority of the institutions do not publish any part of the awards: only one of them states that "decisions, complaints, and supporting materials will be posted publicly unless otherwise ordered by the arbitrator" (but this has not happened yet), and three of them publicize statistical, aggregate data or anonymous summaries of cases. Nevertheless, two institutions offer the possibility to publicize the results of the cases, if the parties agree to do so, but this possibility has not been used yet.

Only one type of ODR providers publicize the results with many details: all dispute resolution providers which operate under ICANN Uniform Domain-Name Dispute Resolution Policy are required to publicize all decisions in full text on the Internet, except when a panel decides otherwise, which can occur in exceptional circumstances. The publications mention the parties, and are rather extensive (usually 1500-2000 words).

Globally, these reflections and the survey show that the publication or the confidentiality of documents are of high concern to all parties invovled in online dispute resolution. All documents, in ODR, can be classified in different 'categories of sensibility', depending on the harm that their involuntary publication could cause on the parties. Different levels of protection correspond to these different levels of sensibility. From a technical point view, there are several technological mechanisms that could provide the appropriate levels of protection. These mechanisms are analyzed hereafter.

ODR and communication from technical point of view

In this part, we first outline the security needs due to the use of electronic documents. Then, we present the technological tools involved in managment of data and communication. Finally, we discuss some properties that seems important for ODR systems.

Security needs

One of the major advantages of e-commerce is that there is no paper, that electronic data benefit from many of these tools that made computers a revolution. Still, electronic data management and communications also show important drawbacks. It is for instance widely acknowledged that unprotected email and web-based communications are more vulnerable than communications by paper documents. If ODR providers state that the collected information is treated confidentially, this does not necessarily imply that such information cannot be transmitted or accessed accidentally or that it cannot be accessed by third parties. It is nowadays commonplace that electronic messages need to be protected by electronic means, and that electronic communication and the access to the data must be secured, before, during and after the ODR procedure.

In addition to the protection of data and communication support, it is important to protect the data processing. For instance, concerning the confidentiality, it is not sufficient to ensure the confidentiality of the data itself but it is necessary to treat the data confidentially (for example

concerning the publication of dispute cases).

The protection of electronic communication and data is also a prerequisite for very important issues like:

- evidence in dispute resolution: the documents exchanged between a mechant and his customer oftern constitues the only evidence for the conclusion and performance of the contract, and if such a document is likely to have been faked, it will hardly be accepted as evidence by dispute resolvers, or
- trust: the end-user has to be ensured that the mechanisms needed for the protection of the relevant data are actually used.

These issues are beyond the scope of this paper, but they underpine many of the following sections.

Communication and Data Protection

During the initial developments of IT communication tools, the primary focus was placed on functional capabilities - security was a secondary issue. A long list of requirements needs to be met to raise electronic communication tools to the level of trustworthiness of traditional means.

Several products and protocols which address these issues have been developed, but they are neither fully satisfactory nor used on a large scale. Since security is lacking in the electronic data processing infrastructure, it becomes particularly important to recognize and define responsibilities.

Protecting information has two aspects: the transmission and the storage of information. These two aspects require different means of protection but are exposed to identical risks: unauthorized third parties must not be capable of accessing the information (which means protecting the *confidentiality* of a message) and, a *fortiori*, altering this information (which means protecting the *integrity* of a message).

Protection of email

Standard, unencrypted email is considered, and rightly so, to be about as secure as postcards [58][59]. Standard emails clearly do not meet the requirements of the protection of the confidentiality and integrity of the information.Emails can be secured by several means (some of which being available free of charge) that are set out below.

Secure Multipurpose Internet Mail Exchange Protocol (S/MIME)

A system for message protection that has a strong vendor acceptance and has already been deployed on several well accepted email products is the Secure Multipurpose Internet Mail Exchange Protocol (S/MIME) [60]. This protocol makes it possible to authenticate the origin of the email, and to ensure the confidentiality and integrity of its content. If S/MIME is correctly used, the risk of successful repudiation by the apparent sender during litigation is very low, as S/MIME provides a recipient with strong evidence of the origin or content of a message.

In addition, S/MIME also offers Message Confirmation Services: it informs the person who sent the message that it has been delivered to a recipient or at least reached some specific point on its path. In other words, S/MIME provides evidence of delivery. However, this requires that the sender and every recipient obtain a certificate, which must be paid for.

Others solutions of security enhancement exist, such as Pretty Good Privacy (PGP) [61], a

message-protection software which is popular within various niches of the Internet community and available from the Massachusetts Institute of Technology (MIT). It provides the same quality of service as S/MIME. This solution is free of charge since its development has been done as open source. However, PGP has a severe drawback: it is difficult to deploy for use by non-specialists. PGP defines its own non-standardized Public-Key Infrastructure (PKI) [62], based on mutual trust rather than a formally established authority.

Digital Signatures

The risk of repudiation and alteration of a message can also be reduced by digital signatures. They are cryptographic instruments generally attributed by trusted private or public certification authorities (CA) to previously identified persons (signature or key holders). The receiver of an electronically signed message can verify both the origin and the integrity of the message. By using a public counterpart of the private and secret signature, the receiver is able to check whether the private signature of the sender has actually been used to sign the message. On request, the CA provides information about the signature/private key used. If the key of the apparent sender has been used in order to create the signature, a dispute resolver is most likely to hold that the message is attributable to the sender/holder of the private key that was used.

Digital signatures can also be used to prove the receipt of the message. If the addressee simply replies to the message by signing it electronically, the sender can prove that the original message has been properly received.

In order to document the moment at which a document was sent, the CA can place an electronic time stamp or watermark on the document. If the technology is implemented in the computer of the sender, it must however be ascertained that the sender cannot temper with the mechanism (black box).

At a technical level, solutions to this problem exist and are beginning to be available. However, those solutions require an authority of trust, which in turns requires an established infrastructure.

Protection of web-based communication

When information is communicated by being posted on a web site, instead of being communicated by emails, different means of protection have to be used. For instance, when a submission form is distributed directly through a web site, a specific protection mechanism is needed.

The *Hypertext Transfer Protocol* (HTTP) [63] has become the generally accepted transmission protocol for online transactions. Several methods for securing web-based communications are used to supplement HTTP, the most frequent being the *Secure Sockets Layer* (SSL) [63]. SSL-secured HTTP provides protection of the confidentiality and the integrity of the data transmission.

The fact that SSL is used on a web site is indicated by a URL beginning with HTTPS, instead of HTTP. In order to indicate a secured site, a specific symbol appears in the status bar at the bottom of the window (e.g. closed lock or a solid key symbol, unless a navigator is used that does not follow the conventions on indicating secured and non-secured zones).

However, HTTP is not the only protocol used to exchange data. There are alternatives, for instance "*applets*" which have a high potential for securing communications, but are not yet sufficiently deployed. This is particularly true in existing ODR environments.

Protection of stored data

The record management and the data protection is applied locally at each site (as opposed to the network). ODR system providers have to protect both their storage site system (database and web server) and each individual record and its related data. This protection aims at such risks as virus infections, intrusions, or disk crashes.

The protection of the storage site systems can be implemented by firewalls (which thus also protect the individual records). Specifically for disk crashes and virus infections, means are available as such backup policies and intrusion detection systems against attacks.

However, as was mentioned above, it is safer to implement the protection at the level of each individual record, and then protecting the system as a whole.

Summary

The survey shows that current ODR systems rarely use secured emails. Submissions via web sites normally offer better support for security.

Globally, it is more efficient to protect the transmitted data than the communication channel. Protecting the transmitted data ensures the integrity of the data from origin to storage, regardless of the media used for the communication and processing.

Some technical requirements for ODR systems

In addition to the protection aspects, some properties are essential for ODR systems [64]. The following are considered to be the most important.

- **Communication mechanisms**

  ODR Systems have to support specific kinds of human interaction, for instance email exchanges, voice communications, videoconferences; as we have seen, they also have to allow private communication sessions (caucus). Some ODR providers offer online chat-rooms and threaded discussion (caucus-like) capabilities [65], and even audio flow synchronization problem management.

- **Availability and timely response**

  Computer systems and communication facilities must be performing sufficiently well to avoid "sluggish response" to the end-user. This also implies that the ODR systems provide for quantifying the system response (e.g. "transaction per time unit") and define upgrade mechanisms. Moreover, the supported process must be efficient from the point of view of the user. The parties must, for instance, be able to have a feedback on the state of the process, for reasons of transparency and for accelerating the procedure. Another means for accelerating the process is the synchronization of several procedures involving the same complainer or defendant. This can be achieved by *user case rooms* and *aggregated case data*.

- **Simplicity**

  Users must be able to follow the state of the process. For this reason, ODR system providers have to pay attention to: a) the quality of the system and the user interface (they have to provide clear information about the progress of the process), and b) the implementation must respect standards provided by high-quality conventions for user

interactions (the underlying support architecture must correspond to established configurations and standards).

- **Adaptability**

  A system is considered to be *adaptive* if it can automatically and "intelligently" adjust itself to new conditions of interaction with users. *Adaptative* systems can take care of "user profiles" and the user's capacities or disabilities to follow a process. The World Wide Web consortium addressed this problem with the *Web Accessibility Initiative* (WAI) [66]; nevertheless, this solution is not sufficiently deployed in e-commerce and, more specifically, in ODR. The major drawback of such a system is a loss of privacy, because the system is aware of the characteristics of the user. This awareness can be used for collecting data on the users, and they can of course be misused, for instance for commercial purposes. This problem is one of the concerns of the *Privacy and P3P Initiative* [67] of W3C. In addition, since the procedures must be available to as many parties as possible, ODR system providers must carefully define the required equipment and the software platform. This issue raises questions ranging from the support of videoconferencing to the consideration of problems related to time zones.

- **Interoperability**

  Information needs to be stored, for instance as evidence and for purposes of general data management. When such data is communicated from site to site, the issue of a standard exchange system arises.

ODR providers, online merchants and courts must cooperate and, to this effect, they must exchange information. Thus, data exchange standards have been implemented, so-called *Exchange Markup Languages* (XML [68], and in the ODR context ODR-XML [69]). The Joint Research Commissions (JRC) [69] of the European Commission is currently working on the development of an ODR-XML, the latest step in the process being the launching of *the Demonstrator*[70]. The Demonstrator allows a user to "file a new case with notification mail to the respondent (claimant), respond to a case (claimant and respondent), view case(s) (claimant and respondent), and finally export a case in XML". The Demonstrator thus experiments the interoperability and transferability of cases by using an ODR-XML .

A predecessor of the Demonstrator is *CLAIM*, another initiative of the JRC, which was part of the first XML effort, in 1998: the *World-Wide-Web Consortium* (W3C) proposition entitled *XFDL* (Extensible Forms Description Language) [71]. It experimented with electronic records that provide non-repudiation evidence by linking form questions to form answers, thus providing evidence of the context of the agreement. No provider, however, presently uses any such XML technology.

Conclusion

The impact of electronic handling and communication goes beyond management and security: electronic communication may constitute evidence to be submitted to an arbitrator or a court . If, for instance, a dispute arises between a buyer and a seller over the existence or the terms of a contract concluded electronically, one of the parties may have to prove the conclusion of the contract (that is the reception of the offer or the acceptance by the adressee) and its contents.

If no specific tools were used, the parties may easily argue that an email was forged or that the information of the web page, for example the information about standard terms, has been altered since the conclusion of the contract. A debtor of a merchant may, for example, claim that a

malevolent third person, who came to know about the beginnings of a contractual relation over the Internet, created an email address with the name of one of the parties, counterfeited its identity and mislead the other party.

Therefore, technological means must be used that rule out any reasonable doubt that data produced as evidence have been altered. This is necessary for two classes of communications: between merchant sites and their users and between the parties and a dispute resolver. Which technological means must thus be available?

In most countries, a dispute resolver can assess the weight of the evidence and, for instance, evaluate emails by comparing them with other sources of evidence, or by comparing them among themselves: if a series of emails includes each time the original message replied to, a certain factual presumption arises. However, there is a need for special rules on the concluding force of electronic documents.

The non-repudiation of a message can be ensured, for example, by the use of particular software protocols (for instance the S/MIME protocol) or by digital signatures, as set out above. Another solution is to send a copy or reference of every communication that could become litigious to a third neutral party, for instance an electronic notary public. This is obviously a more controversial solution.

General recommendations to ODR providers could be articulated in the following simple terms:

- ODR providers must recognize the risks implied by the technology they use; they must take the necessary measures to reduce them and have a clear policy regarding the remaining risks. This means that the customer has to be informed both about the risks and the possibility to reduce them to an acceptable minimum.

- ODR providers must place particular emphasis on issues specific to dispute resolution such as data integrity and protection, system simplicity and accessibility; they must use technical solutions capable of protecting the strategic nature of the information being handled.

ODR providers must ensure the compatibility of their system with those of both merchants and customers, so that electronic evidence can easily be produced. They must agree on a standard of representation (data, record and data exchange models) of documents, for example a standardization of protocols. This standard minimizes efforts of handling and conversion of these documents between the parties that interact with ODR Systems. Besides, it will allow ODR providers to adapt their internal representation to requirements of external communication and exchange. In the long run, an integration of solutions used in e-commerce and ODR is likely to be central.

Perspectives

Having discussed the technological aspects, which are relevant to ODR systems, we now outline some perspectives concerning the impact of the future of the Web (such as Semantic Web, Web services,...) on ODR systems from a standardization point of view, and vice-versa. The technological tools presented previously result from standards developed for the Internet and the Web. Actually, in our work, we focus mainly on IETF and W3C standards, because of their large deployment. In addition to these standardization organisations, we could consider other standardization initiatives undertaken by other actors such as dispute resolution providers, consumers, industry, government (for example the JRC initiative concerning ODR-XML).

ODRs as Web services

The Web could be seen as a marketplace, where services are provided to consumers over the network. ODR should be considered as an important service for electronic commerce and business. Until now, we focused on communication protocols and message formats (XML, HTTP,...) standardized by the Web community. However, it is important to consider the service aspect. Actually, users have to be oriented toward the appropriate service to fulfill their requirements. In the context of dispute resolution, it is important for the complainant to find the appropriate ODR provider to treat his claim. One solution is to use Web-Services Description and Localisation (WSDL) [72]. The aim of WSDL is to address this issue, in conjunction with SOAP 1.1, HTTP GET/POST and MIME protocols and standards. WSDL is *an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information*[72]. This last point is appropriate for management of online dispute resolution cases, which are involved in workflow processes. WSDL is one proposal and other proposals are to use the Semantic Web for description and discovery of Web services.

ODR with a specific ontology

From the perspective of building a Network of Knowledge, each service provider has to explain its objectives and capabilities. From a legal point of view, the law community has to deal with the integration of legal concepts in electronic commerce and in the electronic environment of the user community. The legal world has its own traditional ontology that it has not really been mapped into those of the electronic world. Specifically, ODR-XML deals with the descriptive syntax of a claim but less with the semantics of the legal terminology. However, the semantics are important in order to automate the ODR processes (i.e. negotiation, mediation, arbitration). The Semantic Web is a possible way for fulfilling this requirement. Actually, the Semantic Web is defined by W3C as *the idea of having data on the web defined and linked in a way that it can be used by machines not just for display purposes, but for automation, integration and reuse of data across various applications* [73].

References

1. C. HART, "Online Dispute Resolution and Avoidance In Electronic Commerce". Draft Report, August, 1999. http://www.law.ualberta.ca/alri/ulc/current/hart.htm [2]

2. C. SEBASTIAN. "eResolution". Press Release, July, 2000. http://www.eresolution.com/pr/06_07_00.htm [3]

3. T. SCHULTZ, G. KAUFMANN-KOHLER, D. LANGER, V. BONNET, J. HARMS. "Online Dispute Resolution: State of the Art, Issues, and Perspectives". Draft Report, Faculty of Law and Centre Universitaire Informatique, University of Geneva, October, 2001. [4]

4. American Bar Association Task Force on E-commerce &Alternative Dispute Resolution, Draft Preliminary Report & concept paper, May, 2001. http://www.law.washington.edu/ABA-eADR [5]

5. E. KATSH and J. RIFKIN, "Online Dispute Resolution: Resolving Conflicts in Cyberspace", San Francisco, CA, Jossey-Bass, 2001. [6]

6. J. MELAMED, "Integrating The Internet Into Your Mediation Practice". White paper, November, 2000. http://www.mediate.com/articles/melamed8.cfm [7]

7. VAHRENWALD, "Out-of-court dispute settlement systems for e-commerce. Report on legal issues. Part III : Types of Out-of-Court Dispute Settlement", report of the Joint Research Center of the European Commission, 29th may 2000, http://econfidence.jrc.it/default/show.gx?Object.object_id=EC_FORUM0000000000000FF0. [8]

8. R. P. ALFORD, The Virtual World and the Arbitration World, in Journal of International Arbitration, 18(4) : 449-461, 2001. [9]

9. VAN DEN BERG, "The New York Convention of 1958", 1st ed., London, Kluwer Law and Taxation Publishers, 1981, p. 44 ; A. REDFERN and M. HUNTER, "Law and Practice of International Commercial Arbitration", 3rd ed., London, Sweet & Maxwell, 1999, p. 3-4; A. BUCHER and P.-Y. TSCHANZ, "International Commercial Arbitration in Switzerland", Basle, Helbing and Lichtenhahn, 1989, p. 26. [10]

10. VAHRENWALD, "Out-of-court dispute settlement systems for e-commerce. Report on legal issues. Part IV : Arbitration", report of the Joint Research Center of the European Commission, 31st October 2000, http://econfidence.jrc.it/default/show.gx?Object.object_id=EC_FORUM0000000000000FF9. [11]

11. http://www.123settle.com [12]

12. http://www.allsettle.com [13]

13. http://www.clicknsettle.com [14]

14. http://www.cybersettle.com [15]

15. http://www.intersettle.co.uk [16]

16. http://www.resolvemydispute.com [17]

17. http://www.newcourtcity.com [18]

18. http://www.resolveitnow.com [19]

19. http://www.settlementonline.com/Index.html [20]

20. http://www.settleonline.com [21]

21. http://www.settlesmart.com [22]

22. http://www.theclaimroom.com [23]

23. http://www.ussettle.com [24]

24. http://www.webmediate.com [25]

25. https://www.wecansettle.com [26]

26. https://www.claimchoice.com/Public/PublicHomepage.jsp [27]

27. http://www.ecodir.org [28]

28. http://www.ilevel.com [29]

29. http://www.onlineresolution.com [30]

30. http://www.resolutionforum.org [31]

31. http://www.squaretrade.com [32]

32. http://www.truste.org [33]

33. http://www.which.net/webtrade [34]

34. http://www.cybercourt.org [35]

35. http://www.consensus.uk.com/e-mediator.html [36]

36. http://www.eresolution.ca [37]

37. http://www.intellicourt.com [38]

38. http://www.internetneutral.com [39]

39. http://www.ecp.nl/trust/index1.htm [40]

40. http://aaron.sbs.umass.edu/center/ombuds/default.htm [41]

41. http://www.onlinedisputes.org [42]

42. http://www.novaforum.com [43]

43. http://www.settlethecase.com/main.html [44]

44. http://www.webassured.com [45]

45. http://www.webdisputeresolutions.com [46]

46. http://www.webdispute.com [47]

47. http://www.vmag.org [48]

48. http://www.wordandbond.com [49]

49. J. HAYNES. "Metaphors and Mediation". Mediate.com, http://mediate.com/articles/metaphor3.cfm. [50]

50. BEVAN. "Alternative Dispute Resolution". London, Sweet & Maxwell, 1992, p. 31. [51]

51. R. S. GRANAT, "Creating An Environment for Mediating Disputes On the Internet". [52]

52. DUVAL SMITH. "Problems in Conflict Management in Virtual Communities", in Communities in Cyberspace, P. KOLLOCK et M. SMITH (ed.), Routeledge Press, 1998. [53]

53. G.R. SHELL. "Computer-Assisted Negotiation and Mediation: Where We Are and Where We Are Going". In Negotiation Journal, 11(2), p. 117-121. [54]

54. REDFERN and M. HUNTER, Law and Practice of International Commercial Arbitration, 3rd ed., London, Sweet & Maxwell, 1999, p. 311-338. [55]

55. in G. KAUFMANN-KOHLER and H. PETER, Formula One Racing and Arbitration: The FIA Tailor-Made System for Fast Track Dispute Resolution, in Arbitration International, Vol. 17, No. 2, 2001, p. 173-210. [56]

56. E. KATSH, The Online Ombuds Office: Adapting Dispute Resolution to Cyberspace, A Working Paper for the NCAIR Conference on ODR, Washington, DC, May 22, 1996, http://mantle.sbs.umass.edu/vmag/disres.html. [57]

57. J. PAULSSON & N. RAWDING, The Trouble with Confidentiality, in Arbitration International, Vol. 11, No.3, 1995, p. 303. [58]

58. T. LAPP. "Fax und E-mail-Kommunikation". http://www.dr-lapp.de/faxmail.htm. [59]

59. M. HORAK. "Das Internet im Zeitalter des eCommerce". http://www.iprecht.de/Home/Gebiete/Computer/Internet/eCommerce/eVertrag/body_evertrag.html. [60]

60. http://www.imc.org/smime-pgpmime.html [61]

61. PGP definition at http://web.mit.edu/network/pgp.html [62]

62. ftp://ftp.ietf.org/rfc/rfc2693.txt [63]

63. http://www.w3.org/Protocols/ [64]

64. M.Wilikens, A. Vahrenwald, P. Morris. "Out-of-court dispute settlement systems for e-commerce.- Report of an exploratory study", Joint Research Centre, Ispra - Italy, 20th April, 2000. [65]

65. http://www.resolutionroom.com/ of Onlineresolution. [66]

66. http://www.w3.org/WAI/ [67]

67. http://www.w3.org/P3P/ [68]

68. http://www.w3.org/XML/ [69]

69. http://www.jrc.org/ [70]

70. http://odr.jrc.it [71]

71. http://www.w3.org/TR/NOTE-XFDL. [72]

72. http://www.w3.org/TR/wsdl [73]

73. http://www.w3.org/2001/sw/