Information Disclosure and the Online Customer Relationship[1]

Bruce Jay Forman
New Jersey Institute of Technology
IS Department
bforman13@comcast.net
908-769-8126

Brian Whitworth
New Jersey Institute of Technology
IS Department
bwhitworth@acm.org

ABSTRACT

The issue of eliciting personal information poses ethical and social issues for the designers of electronically mediated human-human and human-organizational information systems. Equally personal information disclosure is central to online trade, because customers who cannot be convinced to disclose cannot trade, as without details like delivery address and credit card there is no trade. A participant's willingness to disclose personal information is an important indicator of trust, as every e-business transaction requires some disclosure, like name, address and credit card. This paper considers the factors that affect disclosure in an online environment, and suggest three: privacy contract, reciprocity and disclosure type. Initial data suggests that disclosure is affected by the type of information requested.

Author Keywords

Online Customer Relationship, Information Disclosure, Trust, Risk.

ACM Classification Keywords

Human Computer Interaction.

INTRODUCTION

Social ability may be as important as intellect in enabling technology to create prosperity. Science for example is as much a collegial effort as an intellectual one. Most, if not all, researchers stand on other's shoulders, and it is hard to imagine science without knowledge sharing. Without a sense of social good, there would be no value to donating scientific discoveries to the public domain. If social values help progress, they can also help technology progress.

The Internet exemplifies the benefits and dangers of social interaction, giving E-bay and Google along with pornography, spam, scams, spoofs, viruses, identity theft, privacy loss and copyright theft. Spam illustrates how technology without social values can be counterproductive [38]. It is an example of the problems rational utility analysis faces when applied to social interaction [37]. Yet social complexity did not begin with the global Internet, and its answer has equally deep roots – human social practice. The *social relationship* seems a way for people to reduce social risk, because it represents not just the current transaction but also future transactions. If one party cheats another, they jeopardize the relationship and all future gains. If social values like friendship can link to practical value, the goal of business may be as much about improving the customer relationship as improving products [6].

The customer relationship can be seen as a subset of human relating in general. In analyzing the dimensions of relational communication, the first factor found is usually some measure of understanding the other person. The dimensions along which relationships develop proposed by Gabarro are self-disclosure, knowledge of the other, and reaction predictability [11]. A common relational communication dimension is intimacy, with sub-dimensions of immediacy/affection, receptivity/trust and similarity/depth [3, 34]. A relationship can be seen as two people mutually moving towards each other in terms of disclosure and understanding. We define a relationship as follows:

> A one-to-one, interactive process, involving first recognition, then a developing understanding of the other person, self-disclosure, accompanying arousal and affect, and the carrying forward of this to future encounters [36]

This paper presents concepts and some initial data from a research program into self-disclosure as a useful measure of online relationships, including the customer relationship.

[1] Published as: Foreman, B. & Whitworth, B., 2005, Information Disclosure and the Online Customer Relationship, *Quality, Values and Choice Workshop*, Computer Human Interaction 2005, Portland, Oregon, p1-7.

TRADITIONAL RATIONAL UTILITY MODELS

The Administrative Model of decision-making is a rational utility approach to disclosure that suggests two influences: loss and gain [7]. Since the decision maker always functions in an environment that is partially unknown, a decision maker's willingness to disclose is based on *expected* gain or loss, where:

Expected (Gain/Loss) = Probability (Gain/ Loss) * Magnitude (Gain/Loss)

The expected loss is the perceived risk, which is not always equal to the actual risk. Theoretically, summing the expected values over the set of possible outcomes yields an expected net gain or loss which decides the choice made. Since decision makers have a finite cognitive ability and are usually not completely informed, they may estimate gains and losses, and may choose an early alternative that satisfices most problem constraints, whether optimal or not [7].

The Administrative Model separates the likelihood of gain/loss from its magnitude, e.g. if the typical loss in a plane crash is death, one might conclude that only a few thrill seekers would ever get on a plane, but if the likelihood of a plane crash is low, the risk is also perceived as low. Likewise citizens who play state lotteries know their chance of success is small, but the magnitude of gain is so great they feel it is worth the monetary risk. Studies support the administrative model. Omarzu's Disclosure Decision Model proposes that as opportunity for gain increases, disclosure increases, but as risk increases, disclosure decreases [23]. Jarvenpaa, et. al., hypothesize that high consumer trust manifests as a reduction in perceived risk, which increases a consumer's willingness to disclose and purchase from an Internet store [16].

While such rational risk/gain analysis models explain why people reveal risky information like credit card data to get a valued product, they do not explain why people disclose in situations with no obvious gain, like an online chat room or bulletin board. In other words, why, in the absence of clear utility gains, do people disclose at all?

Social Information Processing

Social Information Processing (SIP) theory [32, 34] states that relational cues transmit by plain text at a slower rate than in rich channels like voice. Hence online relations should require more time to develop, for social information to get through. The relationship would seem as being built up from transmitted data.

SIP theory predicts that people relating online will begin with low relationship measures, but over time (with the transfer of information) will improve to the level of face-to-face groups. However neither the expected initial difference between online and face-to-face, nor the expected development over time, was found [33]. From the beginning, online interactions achieved more positive levels on several dimensions of interpersonal communication than face-to-face groups, and in no case expressed less intimacy [34], contradicting social information processing theory. Despite multi-media predictions, email is still over 90% text, and text messaging rather than vid-phones seems the next "big thing".

Such results suggest rational information analysis models of social relationships are at best incomplete. Relationships seem more than the processing of information in a rational risk/benefit analysis.

A SOCIAL RELATIONAL MODEL

The missing factor may lie in the mutual nature of social interaction – that it always involves two or more parties. This property of relationships can be called interactivity or reciprocity. Interactivity has been defined as the average rate of change of sender/receiver roles for related messages [28], quickness of feedback [8, 19], or reciprocity/equality of participation [29]. We take it as the degree to which control of the interaction is shared, however all these definitions have a common property: that the deciding party is not a singular entity. This means that the rational analysis of a single entity cannot encompass the outcome.

If relating is both expressing yourself as an individual, and understanding another as the same, it requires shared control, e.g. a turn based action sequence. If disclosure creates risk, one-sided disclosure creates one-sided risk. Interactivity means both parties can risk equally. Each can make adjustments according to the other's response, e.g. to hold back if there is no reciprocal disclosure. Friendship, as a mutually reciprocated affect, requires an interactive situation, as does mutual understanding. The Social Penetration Model proposes that relationships involve a systematic process of mutual self-disclosure, progressing from superficial to deeper areas of exchange [2]. The circular nature of the interaction is shown in (Figure 1).

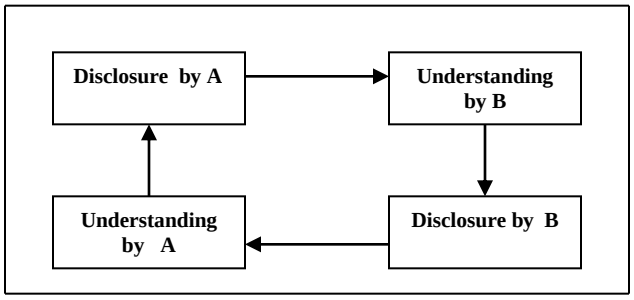

Figure 1 – The Social Penetration Model

This model stretches the normal causal models of science. Self-disclosure measures the strength of the relationship, but also causes it, i.e. it is both a dependent and an independent variable. Each party reveals self-data because the other does, given other factors like utility are constant. This explains why in online communication, people may

self-reveal before receiving any information at all from the other person:

> The most striking finding in the current results suggests that when CMC participants are interdependent over time, they adopt more intimate and sociable relational behaviour *from the inception of the interaction*, and throughout. [34]

The dual nature of disclosure suggests that people will reveal self-data to build relationships. The social value of disclosure is that it creates disclosure, which creates a relationship, which creates trust and predictability.

DETERMINANTS OF DISCLOSURE

What are the determinants of disclosure, factors that influence whether an online party discloses personal information? In particular, we consider factors an online retailer could affect, as if a customer chooses to reveal no personal information at all, there can be no trade.

Privacy Contract

The administrative model suggests that if Internet users perceive the risk of disclosure as high, they will not disclose [13]. Internet users consider risk when deciding if a purchase is worthwhile [13]. Decreasing perceived risk will give more disclosure, and so more trade. If the online merchant can convince the user that the risk is less, they will trade more [16,23]. One way to do that is to offer a privacy contract.

The concept of privacy summarizes many of the concerns users have about personal information disclosure. What is privacy? Valued aspects include avoidance of physical harm [35], increased autonomy [25], and the raising of personal dignity [35]. Privacy can enable relationships, as the amount of privacy an individual will sacrifice to a colleague indicates their closeness [12]. By granting its citizens the right to privacy, society empowers them to decide whether to trust each other or not [15]. Finally, individuals can use privacy to protect themselves from harassment for being different [26].

Privacy has two aspects, immediate observation and long-term information storage, or recording. For example one may not object to being observed in public, but may object to being recorded on a videotape. Observational privacy refers to surveillance, whether by an electronic device or the human eye. Informational privacy refers to the types of data that can be stored in databases, and used, for example, to track individuals and groups in society. This includes the corporate use of data for marketing, and the government's use of techniques such as database matching [17]. Although the need for a society (or community) to hold member data is recognized, we fear the ability to store, redistribute and reuse this data by third parties and the government. The commoditization of personal data, and the ability to transport it almost anywhere at a moment's notice has increased the risk of disclosure.

A basic privacy concept is informed consent, which means the observer informs the observed:

- That they are being observed;
- How their personal data will be used;
- Who will have access to their personal data;
- How long the personal information will be kept;
- Consequences of revealing or not revealing personal information.

This information lets the user draw conclusions regarding the degree of risk and the likelihood of loss. In an online setting, a privacy statement declares what is being observed, how it will be used, who can access it, and how long it will be kept. It is a form of a "contract" between the web site owner and the person visiting the site, regarding the disclosure of their personal data. Hence the presence or not of a privacy statement should affect the degree of disclosure.

Relationship Reciprocity

Approximately 63% of Web users that declined to disclose personal data refused to do so because they did not trust the other parties collecting the data [14]. For one party to simply state they are trustworthy, as is done in a privacy statement, has no value if they are indeed untrustworthy. However if the company has a relationship with its customers, it risks that relationship by failing on a contract. Software trust depends on whether the software itself is judged as reliable and competent [24], and bugs, errors and typos in sales Web pages can negatively impact shoppers [9]. However a significant factor beyond software design is the software supplier's credibility, which depends on the supplier's relationship with its customers [4].

In human-to-human interaction, people improve trust levels by building relationships, including interaction rituals of introducing oneself and giving conventional greetings. Central to such rituals is that for others to trust us we must trust them. In trusting another, we disclose information about ourselves, and make ourselves vulnerable to them, but this also increase their trust. If A trusts B enough to disclose personal information to him, then B is more likely to reciprocate:

> "Mutual revelation is a sign of good faith which makes it easier to trust (not unlike a handshake whose origin reportedly was to show that one was not carrying a weapon) [21]."

Reciprocity of information disclosure is a fundamental social form [Ackerman] that reduces perceived risk by a cumulative relating process that builds up over time [3, 5, 20]. In an online setting with few relationships, user risk perceptions may be based on their online experiences, and those of associates they trust [10,31].

If people treat computers as social actors [27], they are likely to reciprocate to online self-disclosure with their own [22]. Therefore if the person who creates a web site shows enough trust in a visitor to disclose personal information, the visitor should be more likely to trust in return, and as a result disclose personal information. Joinson's online test found that those in a reciprocal disclosure condition disclose more information than those in a non-reciprocal condition [18]. It follows that if a vendor releases personal information, especially that which puts them as some risk, the customer will be more likely to do the same. In conclusion, disclosure by one party in a relationship is a determinant of disclosure by the other, and vice-versa.

Type of Disclosure

Whether self-disclosure is an outcome measure or an outcome cause, it has multiple forms. This seems to reflect different types of "self". For example, information about ones physical self, like a photograph, is distinct from information about oneself as a financial entity. Disclosing data like bank account and credit card number, exposes one to financial identity theft and financial loss. In contrast disclosing physical information like a photograph or physical address can lead to physical harm. Table 1 suggests four types of personal identity, each with a distinct disclosure risk, according to the type of "self" exposed (Table 1).

Type	Definition	Information Examples	Possible Harm
Physical	*Physical Being:* Can be seen, touched, heard and exists in a physical place.	Home address Workaddress Photo	Physical Harm: Property Damage Harassment
Community	*Community being:* Held on community records that record status, and can be accessed	Social Security # Birth name and record StudentID# Immigration status Marriage details	Reputation harm: Criminal record Embarassment Expulsion Surveillance
Financial	*Economic being* : Able to access finances via bank records	Credit card Signature Passwords	Financial harm: Misuse of accounts Identity theft
Interpersonal	*Social being:* Connects and communicates with other people person to person (identified) or person to system.	Home/Work/Cell phone Email address Personal web site Online persona	Nuisance Related: Telemarketing Obscene phone calls Being ostracized Spam

Table 1: Types of Personal Information Disclosure

Exposing a personal address could lead to a physical attack and even death. Exposing one's social security number lets people investigate social information on births, marriage, taxes or even a criminal record. Exposing ones financial self can result in financial loss, while exposing an email or cell-phone number could lead at worst to spam or verbal insults. Clearly the degree of risk varies with type. Physical dangers seem the greatest, followed by community and financial information, then social communication, where the risk is generally inconvenience rather than danger. One can always get a new telephone or email address, but the nuisance factor may still be enough to prevent disclosure. If one creates an online persona (distinct from one's offline identity), such as a character in a virtual game, it may be normal for it to "die" after a while. Yet still it could be a loss one might try to avoid.

Given the previous discussion, type of disclosure can have two effects. Firstly, disclosures that involve greater risk should be less frequent. Internet participants should be less willing to provide personal information that can result in greater harm, e.g. less willing to release their home address than their e-mail address. Further, the more information uniquely identifies the self, the greater the probability it could result in harm, and so the less likely it should be released. For example one should be less likely to release social security or credit card numbers than less identifiable information such as name or gender. [1]. Information perceived as high-risk should be disclosed less than information perceived as low risk.

Secondly, disclosures that involve greater risk should create greater trust, as measured by other disclosure. For example disclosing things like a physical address and photographs of staff will create more trust than disclosing emails.

Preliminary Study

In the above analysis, the concept of disclosure type is new. Hence a preliminary study of 31 people was conducted at a large financial organization to validate the concept. A questionnaire posed a hypothetical situation, where each user was a participant in an online bulletin board populated by securities industry professionals. There was no monetary or specified gain. Users were experienced in online interaction, so the social risks of Internet disclosure were presumed. Each person surveyed was asked whether or not they would voluntarily disclose the following personal information (yes/no answers only); name, home address, home phone, work phone, cell phone, personal email, work email, and personal photograph. A summary of the results is shown in Table 2.

Name	Personal Email	Work Email	Work Phone	Home Phone	Home Address	Cell Phone	Photo
51%	41%	41%	35%	10%	8%	6%	6%

Table 2. Disclosure by Information Type

These results support the idea that disclosure varies with disclosure type (Chi-squared $p < 0.001$). Participants were more willing to disclose their name, personal and work email, and work phone than home phone, cell phone, home address or photograph. Theory predicts that personal information that can produce greater harm should yield less disclosure. Home address and photograph could lead to

property damage or physical harm, and are infrequently disclosed. Participants showed the least reservation in disclosing their name, perhaps because names are not unique, and knowing the name of an individual is not enough to locate them, or even define them in a community. Email and work phone were also readily disclosed, presumably because users did not feel threatened by email or telephone calls at work. Home phone was much less readily disclosed as telephone risks like obscene phone calls or telemarketing are more of a problem at home. People may feel safe from harm at work, or see telemarketers as wasting the employer's time rather than the person's time. Participants were particularly unwilling to release cell phone information. Since the risk exposure was only communicative, the model suggests the reason to be probability, i.e. people carry cell phones at all times so are more likely to be disturbed in person.

These results suggest that disclosure type affects degree of disclosure, and warrant further research.

5.0 CONCLUSIONS

The issue of eliciting personal information poses ethical and social issues for the designers of electronically mediated human-human and human-organizational information systems. One solution is to provide users with the information they need to make disclosure decisions, e.g. a privacy contract. Another is the social approach, of mutual disclosure and mutual risk. In this social model, disclosure is mutual, so both parties engage risk equally. Both models are modified by the type of disclosure, which relates to the type of self disclosed, namely physical, community, financial and social.

Personal information disclosure is central to online trade, because customers who cannot be convinced to disclose cannot be convinced to trade. Building an online customer relationship requires reciprocity, and unless this is done, the vendor is undefined. A customer who reveals nothing, not a name, nor an address, nor a credit card number, is not a customer at all. Hence the determinants of online disclosure are very much also the determinants of online trade. Our analysis suggests three factors:

1. Privacy contract
2. Vendor disclosure
3. Disclosure type

The vendor must tell customers what will happen to any personal data they reveal to the company. If this is not done, the risks are undefined.

The vendor must offer information to match that requested from the customer, like an address, telephone number or email. Since home address is necessary for product delivery, this may explain the recalcitrance of customers to trade online. The relative success of "brick and mortar" merchants in online trading may be because customers have the company's physical address. Internet users are often just "visitors", who use the Web, but do not participate significantly in any online interaction that requires them to divulge personal information. Until this group of "viewers" is converted to participants rather than visitors, the value of the Internet will not be realized.

> "Millions of consumers browse thousands of web vendor sites everyday with the intention of buying products and services. Yet, the majority of these consumers opt for buying the products or services from a brick-and-mortar facility rather than completing the purchase process online [30]"

By revealing a local delivery address, brick and mortar suppliers may be satisfying the social requirement of reciprocal disclosure.

Finally, vendors must carefully consider the information they ask for in on-line transactions. Asking for cell-phone or home phone may require a significantly higher level of user risk than just email. If vendors wish more risky data from customers, they may need to consider giving customers more data about their organization, like staff names and extension numbers.

In conclusion, the mutual nature of social interaction introduces a dimension beyond risk analysis that affects self-disclosure, namely shared disclosure. In addition, disclosure can be categorized by the type of self disclosed, which affects both rational and social models of self-disclosure. Further research may clarify the complex relations between these factors.

6.0 REFERENCES

1. Ackerman, Mark S., Cranor, Lorrie Faith, Reagle, Joseph, Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences, ACM, 1999
2. Altman, I and Taylor, D. A., Social Penetration: The Development of Interpersonal Relationships, Holt, Rhinehart and Winston, 1973
3. Burgoon, J. K. and Hale, J. L., The Fundamental Topoi of Releational communication, Communication Monographs, 51, 193-214, 1984.
4. Cassell, Justine and Bickmore, Timothy, External manifestations of Trustworthiness in the Interface, Communications of the ACM 12/2000, Vol 43, No. 12
5. Castelfranchi, Cristiano and Tan, Yao-Hua, The Role of Trust and Deception in Virtual Societies,Proceedings of the 34th Hawaii International Conference on System Sciences, IEEE, 2001
6. Customer Relationship Management, http//guide.darwinmag.com/technology/enterprise/crm.
7. Davis, Gordon B. and Olson, Margrethe H., Management Information Systems Conceptual

Foundations, Structure, and Development, 2nd Edition, Pps 170-183

8. Dennis, A. R., Valacich, J. S. and Nunamaker, J. F. Jr., An Experimental Investigation of Group Size in an Electronic Meeting System Environment, IEEE Transactions on Systems, Man, and Cybernetics, 20(5), 1049-1057, 1990.
9. Fang, Xiaowen and Salvendy, Gavriel, Customer-Centered Rules for Design of E-Commerce Web Sites, Communications of the ACM, December 2003, Vol46, No. 12ve
10. Friedman, Batya, Kahn, Peter H., Howe, Daniel C., Trust Online, Communications of the ACM 12/2000, Vol 43, No. 12
11. Gabarro, J.J., The Development of Working Relationships, in J. Galegher, R. Kraut, C. Egido, Intellectual Teamwork, Lawrence Erlbaum, 79-110, 1990
12. Gavison, Ruth, Privacy and the Limits of theLaw, The Yale Law Journal, Vol. 89, No. 3, Jan. 1980.
13. Gefen, David, Rao, V. Srinivasan, Tractinsky, Noam, The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarification, Proceedings of the 36th Hawaii International Conference on System Sciences, IEEE, 2003
14. Hoffman, Donna L., Novak, Thomas P., Peralta, Marcos, Building Consumer Trust Online, Communications of theACM, April 19999, Vol. 42, No. 4
15. Introna, Lucas D., Privacy and the Computer: Why We Need Privacy in the Information Society, Metaphilosophy, Vol. 28, No. 3, July 1997, Pps 259-275.
16. Jarvenpaa, Sirkka L., Tractinsky, Noam, and Saarinen, Lauri, Consumer Trust in an Internet Store: A Cross-Cultural Validation, JCMC, December 1999, Volume 5, Issue2.
17. Johnson, Deborah G., Computer Ethics, Simon and Schuster, 1985, p95.
18. Joinson, Adam N., Knowing Me, Knowing You: Reciprocal Self-Disclosure in Internet-Based Surveys, Cyber Psychology & Behavior, Volume 4, Number 5, 2001.
19. Kraut, R., Galegher, J., Fish, R., and Chalfonte, B. Task Requirements and Media Choice in Collaborative Writing, Human Computer Interaction, 7, 375-407, 1992.
20. Kristoffersen, Steinar and Ljungberg, Fredrik, An Emprical Study of How People Establish InteractionL Implications for CSCW Session Management Models, ACM CHI 1999
21. Marx, Gary T., Idnetity and Anonymity: Some Conceptual Distinctions and Issues for Research,From Caplan, J., and Torpey J., Documenting Individual Identity, Princeton University Press, 2001
22. Moon Y., Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers. Journal of Consumer Research, 27:323-339.
23. Omarzu, Julia, A Disclosure Decision Model: Determining How and When Individuals Will Self Disclose, Personality and Social Psychology Review, 2000, Vol. 4, Issue 2, Pps. 174-185
24. Papadopoulou, Panagiota, Kanellis, Pangiotis, Martakos, Drakoulis, Investigating Trust in E-Commerce: A Literature Review and a Model for Its Formation in Customer Relationships, HICCS, 2001, Pps 791-798.
25. Parent, W.A., Privacy, Morality and the Law, Philosophy and Public Affairs, Vol. 12, No. 4, Fall 1983, pps 269-288.
26. Rachels, James, Why is Privacy Important, Philosophy and Public Affairs, Vol. 4, No. 4, Summer 9175, pps 323-333.
27. Reeves, B. and Nass, C., The Media Equation: How people treat computers, television, and new media like real people and places, 1996, Cambridge University Press/ICSLI
28. Rice 1987
29. Rice 1994
30. Salam, A. F., Rao, H.R., and Pegels, C.C., Consumer-Perceived Rrisk in E-Commerce Transactions, CACM, December 2003, Vol46, No. 12ve.
31. Tyler, Tom R. and Kramer, Roderick M., Whither Trust, From Trust in Organizations Frontiers of Theory and Research, Kramer, Roderick M. and Tyler, Tom R., 1996, Sage Publications
32. Walther, J. B. Interpersonal Effects in Computer Mediated Interaction: A Relational Perspective, Communication Research, 19, 52-90, 1992
33. Walther, J. B., Anticipated Ongoing Interaction Versus Channek Effects on Relational Communication in Computer Mediated Interaction, Human Communications Research, 20(4), June, 473-501, 1994.
34. Walther, J. B., Relational Aspects of Computer Mediated Communication: Experimental Observations Over Time in Computer-Mediated Interaction, Organization Science, 6(2), March, 1995, 186-203.
35. Warren, Samuel D. and Brandeis, Louis D., The Right to Privacy, Harvard Law Review, Vol. IV, No. 5, Dec. 15, 1890, pps 193-220.
36. Whitworth, B., Generating Group Agrement in Cooperative Computer Mediated Groups: Toeards an Integrative Modelof Group Interaction, University of Waikato, Doctor of Philosophy Thesis, Hamilton, New

Zealand, UMI Publication Number: AAT9821071, 1997.

37. Whitworth, Brian, Van de Walle, B., and Turoff, M., Beyond Rational Decision Making. Paper presented at the Group Decision and Negotiation 2000 Conference, Glasgow, Scotland, 2000.

38. Whitworth, Brian and Whitworth, E., Reducing Spam by Clasing the Social-Technical Gap, Computer, October, 2004 .