Can you defend your information in court?

Richard Y. Wang
Massachusetts Institute of Technology
rwang@mit.edu

Yang W. Lee
Massachusetts Institute of Technology
ylee@mit.edu

Diane M. Strong
Worcester Polytechnic Institute
dstrong@wpi.edu

Abstract: Information defensibility is becoming a critical issue to many organizations. We define information defensibility and interpret it in light of the dimensions of information quality. This understanding of information defensibility provides the background for exploring solutions. We explore how information quality and information disclosure policies can support and insure information defensibility. These information defensibility solutions are illustrated via two mini-cases. Addressing information defensibility issues can improve customer relations as well as avoid potentially high legal and financial risks.

1. Introduction

Customers of a chemical company are suing the company for unexpected damages from using the chemicals. Is the chemical hazard information given to these customers defensible? Customers of a brokerage company are suing for investment losses. Is the financial risk information given to these customers defensible? Patients are suing their HMO over a medical treatment. Is the information these patients received about alternative treatments and their risks defensible? If information is not defensible, companies can face severe legal and financial consequences. Under what conditions can these companies defend their information in court?

Information defensibility applies to individuals as well as organizations. The Internal Revenue Service (IRS) is auditing an individual's tax return. Is the information used to make that return defensible?

Defensible information is information that stands up against any scrutiny, such as a legal challenge or formal inquiry. Information defensibility is important to many organizations because of the potentially high liabilities from failing to collect, store, and use defensible information. Examples of organizations with high information defensibility liabilities are:

- healthcare companies that treat patients who have life-threatening diseases;
- environment, chemical, and nuclear companies that dispose hazardous waste;
- tobacco companies that sell products with health risks; and
- financial companies that invest and risk their customers' funds.

Information defensibility is also important to organizations because of its positive impact on sales and customer loyalty. Organizations that fail to address information defensibility issues not only expose themselves to financial and legal risks, but also miss opportunities for improving their relationship with customers.

Legally in the U.S., information falls into two categories [3]. When information is part of a product, it falls under product liability laws. When information itself is a product or service, such as a book or a newspaper, information is protected under freedom of speech and press. The issues examined in this paper address information related to product liability laws. Specifically, we answer three key questions germane to insuring information defensibility under product liability laws:

A. What does information defensibility mean in terms of the dimensions of information quality [6]?

B. How can information quality management insure information defensibility?

C. How do information-disclosure policies support long-term information defensibility?

Answers to these questions illustrate how information defensibility can be interpreted and addressed. First, relating information defensibility to the dimensions of information quality operationalizes information defensibility in terms of its key quality characteristics so that specific solutions can be discovered and applied. Second, information is defensible only if its production meets standards for effective information quality management. Well-documented, consistently-operating information production processes are necessary for meeting such standards. Third, ensuring long-term information defensibility is supported by information disclosure policies. Two mini-cases illustrate

specific instances of how information production processes and information quality management policies affect information defensibility.

2. Interpreting Information Defensibility via Information Quality Dimensions

In our previous research, we identified fifteen dimensions of ***information quality (IQ)*** that apply to organizations and their information [6]. These dimensions define the quality criteria of information that is fit-for-use by information consumers. For any given organization and dataset, however, some of these dimensions will be more important than others.

In articulating the important dimensions of information, organizations relate IQ dimensions in terms of business issues, e.g., information usefulness, usability, and defensibility. Information defensibility is a business issue that can be mapped into IQ dimensions with weighting on these dimensions. Of course, the weightings and the particular dimensions involved will differ across organizations. For any organization and dataset, information defensibility (ID) can be computed as a weighted (w) average over the IQ dimensions (d):

$$ID = \Sigma_{i=1,15}\ w_i * d_i$$

The key IQ dimensions involved in information defensibility are *accuracy, objectivity, reputation, value-added, understandable, interpretable, concise representation,* and *security*[1]. *Accuracy* means that the information is free from errors. *Objectivity* means that the information is unbiased. *Reputation* means that the information comes from reputable and documented sources. *Value-added* means that use of the information improves decision making and performance. *Understandable, interpretable,* and *concise representation* together mean that the information is clear to the person using it. *Security* means that the information is not contaminated by unauthorized access. These together define information defensibility as information that is free of error, unbiased, from reputable and documented sources, valuable and clear to users, and free from tapering.

Other dimensions, such as *timeliness,* may contribute to information defensibility in some situations. For example, when outdated information about a client's risk profile is used for selecting their

[1] Italics are used throughout this paper to indicate an IQ dimension.

investment portfolio, the information is not defensible. In this case, *timeliness* of the information is a component of information defensibility.

The IQ dimensions apply to information as a product that is an outcome of an information production process [1, 4]. To assure high IQ along these dimensions, this process must be well-defined and documented. That is, the information should be traceable through the process and back to its source. A well-defined process is also auditable.

3. Managing for Information Defensibility

Providing for information defensibility begins with a standardized and well-documented process for collecting, storing, and using information. Information is defensible if these activities follow accepted standards. For example, ISO9000 is an accepted standard for quality management of processes and has been applied to ensuring the quality of information products [5]. At a minimum, information defensibility requires the use of a recognized standard, such as ISO9000, for quality information process management.

Quality information process management must be applied to the processes of using information for decision making, as well as the processes for collecting and storing information. In the medical area, for example, when blood is donated, information is collected from donors and the blood is tested for diseases such as AIDS to determine whether the blood is safe for use. Organizations managing the blood supply make decisions daily about the safety of all donated blood. For these decisions to be defensible, the information and processes used to make these decisions must be defensible.

To ensure information defensibility, therefore, organizations must begin with:

(1) setting up standard, consistent processes,

(2) documenting the information collected and used to formulate the decisions,

(3) documenting their processes for collecting the information,

(4) documenting their processes for making the decisions, and

(5) documenting their processes for implementing the decisions.

Providing information defensibility, however, requires more than adopting a standardized process. New evidence that requires changes to the standardized process may arise. In the financial industry, for example, new evidence arises about the risk of derivatives. Investment firms must know these risks, ensure that the brokers who sell financial instruments to customers know these risks, and inform customers. Furthermore, they must document that customers were actually informed of these risks. These issues are currently in the news with Orange County, CA because the county claims that it was not fully informed of the risks involved in its investments.

Implementing information defensibility, therefore, means setting up procedures for collecting information so that the organization is informed about new evidence or situations that may require new actions to ensure information defensibility. Furthermore, extra information must be stored about the information organizations collect, store, and use. For example, information about riskiness must be supplemented with information about when this information was collected, stored, and used and how it was used to make decisions. This is a generalization of the concept of source-tagging in which information about the source (who supplied, when, and how) is carried along with the actual information content [7]. In sum, organizations must:

(6) scan for new information,

(7) analyze new information for potential impact,

(8) revise processes and information products based on the analysis,

(9) document the revisions, and

(10) document all actions taken for information collection, storage, and usage.

These 10 key items form the core of an ***information defensibility strategy***.

4. Information Disclosure

Beyond collecting and storing information according to a defensibility strategy, organizations must ensure that the employees who need to know this information to make decisions about possible changes to current procedures receive this information. This goes beyond *accessibility* to the information.

Accessibility means possible access. For defensibility, access must be required and documented. For example, it is not sufficient to assume that everyone read about junk bonds in the Wall Street Journal; financial companies must distribute information to their customers about the riskiness of specific instruments they invest in.

A component of an information defensibility strategy is an information disclosure policy. An ***information disclosure policy*** specifies who should be informed about what and when they should be informed. Although such policies cover those internal to the organization, a primary focus of such a policy is those external to the company, especially customers.

For example, new investors who bought stock in a company are suing because they were not informed of an upcoming loss expected by the company. As a result of the loss, the stock price declined and investors lost money. The company argues that it was not required to disclose future losses not yet incurred, and furthermore this is internal information that it should not release prematurely.

Another example involves an HMO that is being sued by a patient's family because the HMO failed to disclose the list of treatments and tests it covered. Without this list of information, the patient was unable to assess the information given and tests recommended by the doctor. The patient was not given the appropriate treatment until a covered test indicated the problem. By that time, it was too late for the treatment to be effective. This case is likely to be successful because the courts have continued to uphold a patient's right to know treatment alternatives [2].

These examples illustrate that it is important for organizations to establish an information disclosure policy about what can and should be disclosed to customers. Actions taken based on the policy should be documented. For example, when customers are informed about treatments, what and when they were told should be documented.

The best policy is not necessarily to withhold information. Organizations sometimes believe that customers will not make appropriate decisions if they had full information. This assumes, for example, that doctors are ultimately capable of making decisions for all patients. A policy of providing patients

with sufficient information should be established so that patients can actively participate in making their medical choices.

A well-publicized case of information defensibility and information disclosure policy is the tobacco industry. Since they want to argue that tobacco is not addictive, and even if it were, tobacco companies did not know this, they do not want to document or disclose anything. They do not want to collect, store, or use information that supports a different view.

Ignorance, however, is not a good argument. In the case of the chemical company below, the company was legally responsible because they should have known about the new hazard. Furthermore, trying to hide risks from customers is not a good long-term business strategy, nor is it an ethical business practice. Fortunately, most organizations, like the chemical company discussed below, intend to provide high-quality information to those who need information. Without knowledge of information defensibility, organizations may unintentionally fail to collect, store, and use information appropriately.

5. Two Mini-Case Studies

Two mini-cases illustrate information defensibility in terms of the dimensions of IQ. They also present more specific recommendations for ensuring information defensibility. These cases are composites of several information defensibility incidents from organizations. As such, they should be taken as hypothetical cases developed for illustrative purposes. For example, while a real chemical company did have the information defensibility problem discussed below, the case did not actually involve court actions. These two cases, however, capture the essential aspects of information defensibility issues in organizations.

5.1 Chemical Company

A Fortune 500 chemical company was sued for a problem caused allegedly by one of their chemical products. The suit was successful not because of the problem that occurred, but because of the inadequate information supplied by the company about the chemical. Despite their best efforts to record

and distribute information about known problems related to the chemicals they sell, in this case they failed, and incurred enormous costs. What went wrong? Why was the information they provided about the chemical not defensible?

With each unit of chemical product sold, the company included a material safety data sheet (MSDS) which listed the potential hazards from using the chemical, symptoms of each hazard, and actions to take should the symptoms occur. This MSDS information, if it was *accurate, complete, timely, understandable,* and *adds value* to chemical users, would be defensible in court should one of the known hazards occur. Because of the extremely high costs of not reporting a hazard that might occur, the company had every incentive to provide *accurate, complete, timely, understandable,* and *value-added* information in its MSDSs.

The company had a rational, well-defined process for creating MSDSs. When a new product was developed, the MSDS group contacted experts who knew about the chemical components of the product. These experts helped to write the clauses in the MSDS. There was also a product risk manager who was responsible for risk assessments of the product throughout its life cycle. Every effort was taken to use appropriate experts and to produce an *accurate, complete, timely, understandable,* and *value-added* MSDS.

The problems with the MSDS process occurred in ensuring that the information in the MSDS was up-to-date, i.e., *timeliness* of the information. As the company's products and products from other companies with similar components were used, new evidence of hazards arose. In addition, scientific evidence related to the chemical components in products accumulated as more research was conducted. The company was expected to be aware of new evidence as it arose and to include this evidence in their MSDSs.

In this case, evidence about a new hazard had become available in the scientific literature, but was not included in the MSDS. That is, the link between a known source of *relevant* information, scientific literature, and internal company groups responsible for product risk management and the production of revised MSDSs was broken. The court concluded that the company should have known about this hazard

from the literature and should have included it in its MSDS. Since it did not, the company was liable for damages caused by its chemical.

A related IQ problem in the company was inconsistent updating of MSDSs. A number of their products contained the same chemical components. The hazards of a given chemical component should have been listed as potential hazards of all the products that contained the same chemical. Some product MSDSs were updated, while others were not.

The court had also ordered the company to substantiate the sources of the information in their MSDSs. Unfortunately, they had difficulty in reconstructing the original sources of information for each MSDS. This caused *believability* and *reputation* problems with their MSDS information. Thus, their MSDSs could not be defended in court. Even in cases where the MSDS information was *accurate, complete, timely, understandable,* and *value-added,* it might not be *believable, objective,* or *reputable.*

Given the details about this case, we can now go beyond the general recommendation for a standardized, well-documented process. As suggested in the previous sections, to solve their problems, this chemical company must improve their process of producing MSDS information. Specifically, they needed to set up a standard process for scanning sources of information about the chemical components they used. This included both human experts and scientific literature. For each chemical component, these sources should have been stored in a database along with tracking action information. For example, when was the expert contacted and about what? When was each scientific journal reviewed? Similar procedures needed to be developed for hazards that were reported for their products and, as much as possible, for competitor's products that used similar chemical components. Then in court, they could report their scientific journal review activities and frequency.

For each problem found, they needed to conduct a formal assessment of the potential effect on their product and document the process and results of this assessment. Then in court, they could report this assessment and its scientific basis.

If these assessments resulted in a decision that a hazard was possible, then the appropriate MSDSs should have been updated. This required a database that listed for each chemical component, the

products in which it was used. In addition, the assessment of potential hazard for a chemical component needed to be recorded in the database of chemical components along with the source of that information. Then in court, the source of information for each hazard listed in any MSDS could be easily produced.

Although straight-forward, these recommendations become clear only after analyzing this situation from the information defensibility point of view. Information defensibility is a relatively new problem. The chemical company focuses on producing high-quality chemicals. While its intention is to produce high-quality MSDSs, it did not attend to the information process by which it produces MSDSs in the same way it attended to the manufacturing processes by which it produces its chemicals. The court suit they lost is not caused by poor quality of their chemicals, but by poor quality of their information. Their information was not defensible in court.

5.2 Financial Industry

In the financial industry, customers were sold securities of varying risks. If customers lost money, they could file a complaint with the Securities and Exchange Commission (SEC), which had an arbitration office to settle such complaints. Usually, these complaints were settled in favor of the customer, which meant that the investment company covered the customer's loss. The customer was favored by the arbitration office because the customer felt mistreated and filed the complaint for justifiable reasons; specifically the loss was far more than they were led to expect. The brokers who sold the investment were called investment advisors and they had the responsibility for ensuring that the riskiness of the investment matched the risk profile of the customer. Furthermore, the loss was usually large to the customer, e.g., most of their savings, while small to the investment company. For this reason, investment companies collected risk profiles of their customers and would not approve investments that were too risky for a given risk profile. This was the information they used to defend their sales actions.

The problem the investment companies had was similar to the chemical company's problem with their MSDSs discussed above. They failed to update customer risk profiles on a regular basis. For example, a new computer science graduate with few assets decided to invest some extra cash in Netscape. The investment company built a risk profile for this new graduate. Eight years later when this graduate

had a spouse and several small children, the risk profile of this family had changed substantially. If this family lost $60,000 on its investments, the investment company could be responsible if they had not updated the risk profile and advised the family to switch to less risky investments.

Collecting and updating customer risk profiles is a sound long-term strategy for information defensibility for an investment company. Such a strategy reduces the risk of complaints from customers who feel they were sold investments that were too risky. Furthermore, compiling the risk profile is a sound strategy for increasing sales. An *accurate* risk profile provides the information needed to make good sales. *Accurate* and *complete* information about customers should increase sales, while reducing risks from inappropriate sales. Thus, a strategy for information defensibility can not only reduce legal and financial risks, but it can also be good business practice, e.g., for making targeted sales and retaining customers.

6. Recommendations

With this knowledge of information defensibility, what should an ethical organization do?

First, organizations should treat information defensibility as a strategic issue. Failing to collect, store, and use information based on an established information quality management policy can result in severe legal and financial consequences to organizations. Decisions made now about what information to collect and how to use it could result in extensive legal obligations in the future.

Second, organizations should collect and store information about the sources and uses of their information. This means using well-defined information processes and collecting information about the operation of these processes. It also means making changes and updates to existing procedures as needed to reflect new information and evidence.

Third, organizations should develop a policy that includes what information should be collected and to whom it should be disclosed. This goes beyond current database and data management policies and beyond current attempts to provide high-quality information to information consumers. This policy

should recognize the long-term, strategic importance of information defensibility and the methods of implementing information defensibility through well-defined and documented processes and actions.

By following these three recommendations, organizations will be better positioned to defend their cases in court. Finally, highly defensible information is consistent with highly ethical business practices and can increase profitability by providing more value to customers.

7. References

[1] Ballou, D. P., R. Y. Wang, H. Pazer and K. G. Tayi, Modeling Information Manufacturing Systems to Determine Information Product Quality. Accepted for Publication in Management Science, 1996, .

[2] Leung, S. (1996). Patient has right to know treatment, court says. The Boston Globe, September 4, p. B7.

[3] Samuelson, P., Legally Speaking: Liability for Defective Electronic Information. Communications of the ACM, 36(1) 1993, pp. 21-26.

[4] Strong, D. M., Y. W. Lee and R. Y. Wang, Data Quality in Context. Forthcoming in Communications of the ACM, 1996, .

[5] Wang, R. Y., V. C. Storey and C. P. Firth, A Framework for Analysis of Data Quality Research. IEEE Transactions on Knowledge and Data Engineering, 7(4) 1995, pp. 623-640.

[6] Wang, R. Y. and D. M. Strong, Beyond Accuracy: What Data Quality Means to Data Consumers. Journal of Management Information Systems (JMIS), 12(4) 1996, pp. 5-34.

[7] Wang, Y. R. and S. E. Madnick. A Polygen Model for Heterogeneous Database Systems: The Source Tagging Perspective. in Proceedings ofthe 16th International Conference on Very Large Data bases (VLDB). Brisbane, Australia: pp. 519-538, 1990.