

Globethics Repository



International Review of Information Ethics [vol. 10, 02/2009]

This page was generated automatically upon download from the Globethics Repository.
More information on Globethics see <https://www.globethics.net>. Data and content policy
of Globethics Repository see <https://repository.globethics.net/pages/policy>.

Item Type	Journal
Publisher	International Center for Information Ethics (ICIE)
Rights	With permission of the license/copyright holder
Download date	2026-09-25 21:27:39
Link to Item	http://hdl.handle.net/20.500.12424/175268

Vol. 10 (02/2009)

Business Intelligence Meets Moral Intelligence

edited by Yvonne Thorhauer, Stefan Blachfellner

Editors of this issue:

Dr. phil. Dipl.-Kffr. Yvonne Thorhauer,
Johann Wolfgang Goethe-University of Frankfurt,
Germany
E-Mail: yvonne@thorhauer.org

Mag. Stefan Blachfellner,
INDABA Corporate Consulting, Salzburg, Austria
E-Mail: stefan.blachfellner@indaba-consulting.at

Editors of IRIE

Prof. Dr. Rafael Capurro (Editor in Chief),
University of Applied Sciences, Stuttgart, Germany,
Wolframstr. 32, D-70191 Stuttgart
E-Mail: rafael@capurro.de

Prof. Dr. Johannes Britz, University of Wisconsin-
Milwaukee, USA University of Pretoria, South Africa
E-Mail: britz@uwm.edu

Prof. Dr. Thomas Hausmanninger, University of
Augsburg, Germany, Universitätsstr. 10 , D-86135
Augsburg,
E-Mail: thomas.hausmanninger@kthf.uni-augsburg.de

Prof. Dr. Makoto Nakada, University of Tsukuba,
Japan, Tennodai, Tsukuba, 305-8577 Ibaraki
E-Mail: nakadamakoto@msd.biglobe.ne.jp

Dr. Felix Weil, QUIBIQ, Stuttgart, Germany,
Heßbrühlstr. 11, D-70565 Stuttgart
E-Mail: felix.weil@quibiq.de

Editorial Office

Marcus Apel
Rotebühlstr. 145, D-70197 Stuttgart
E-Mail: MarcusApel@gmx.info

Vol. 10 (02/2009)

Content

Editorial: On IRIE Vol. 10	1
Albrecht Fritzsche: The simulated traces of action - B.I. and reflection through technology	3
Oliver Siemoneit: Business Intelligence and Ambient Intelligence - Some thoughts on the main trends of business information processing, their opportunities, problems and limitations.	9
Paul Wright: Should corporate management include a Computer Forensics and Incident Response capability into realigned Information Security Principles?	15
Roland Bardy and Arthur Rubens: A Comparative View of Business Ethics and Governance in the U.S. and Continental Europe.....	23
Noëmi Manders-Huits and Michael Zimmer: Values and Pragmatic Action: The Challenges of Introducing Ethical Intelligence in Technical Design Communities.....	37
Edward Howlett Spence: The Epistemology and Ethics of Media Markets in the Age of Information	45

Editorial: On IRIE Vol. 10

The inspiration for this special issue began at a conference held in Stuttgart, Germany in December 2007, in which representatives of business and academia, among them experts on business ethics, economists as well as business data processing specialists, discussed the points of convergence between *Business* and *Moral Intelligence*. At this conference it became increasingly clear that the tension between *Business* and *Moral Intelligence* – though of increasing economical, political and social importance – still lacks a thorough scientific investigation.

In addition, in our discussion it became apparent that *Business Intelligence* was defined in terms of an *intelligence agency* for corporations, alluding to the gathering of 'secret' or 'insider-information' about the competitors. Moreover, this definition also spans strategies, processes and technologies used in order to achieve significant knowledge of the status, potential and perspectives of any given business.

However, as this issue shows, there is a broader understanding of *Business Intelligence* that goes beyond the definition shared above. It ranges from technical applications for supporting management decisions, to the quest of information about the actual and potential customers, to designing products that prevent data abuse and to ethical aspects of IT in general. Furthermore, *Business Intelligence* can be understood as a way a company runs its business in an *intelligent* manner, which would be rather *Intelligent Business* than *Business Intelligence*.

Now not only the broader definition of *Business Intelligence* points to some moral aspects. Since technology itself can be viewed as an ethical issue, this also goes for *Business Intelligence* in a narrowly defined sense. Fritzsche demonstrates that the critical potential in which *Business Intelligence* is exposed is when IT becomes "an essential element of the process of decision making itself. With Business Intelligence, we are not only able to decide better or more efficiently. We are able to decide in a completely new way, sharing the authority for our decisions with the technology we use." In this sense "the usage of IT creates an ethical challenge".

One ethical aspect that Fritzsche discusses is that on the one hand technologies need to be simplified so that the user can re-establish his authority over the system. On the other hand this deconstruction diminishes the benefit of technology. Although *Business Intelligence* provides a technological solution for this difficulty, it becomes clear that the problem of the user now shifts to the engineers who have to ensure an adequate simplification of the system.

Like Fritzsche, Siemoneit emanates from *Business Intelligence* in its narrowly defined sense and discusses the impact of Ambient Intelligence on it. Embedding IT-systems in everyday objects leads to ethical issues as well, for instance the loss of privacy by saving personal data on a grand scale. In order to exemplify the various arising problems, Siemoneit refers to the smart factory where individuals come under the domination of machines and the privacy of workers is endangered. Furthermore, he indicates the assets and drawbacks of "Pay-As-You-Drive" models for insurance companies and their clients.

In everyday work-life *Business Intelligence* often goes along with delinquency, especially when it is used for espionage. Wright states that most organisations fail "to recognise all aspects of the security risks that they are exposed to" while at the same time cyber-crime rises because it becomes more profitable the more data is comprised. Besides, organisations focusing on e-crime give attention to detection and prosecution but hardly to prevention and intelligence analysis. The e-crime consultant defines eight innovative measures in order to secure data including the establishment of "E-Crime Departments", a "pro-active hi-tech crisis management so as to identify those who use technology for an unlawful purpose" and procedures which will ensure that any electronic evidence for criminal activities does not get lost.

While there is a broad range of understanding for *Business Intelligence*, the authors agree that *Moral Intelligence* is not the application of morality for business objectives. On the contrary, it describes the willingness and ability to put something else than oneself and something else than efficiency matters in the centre of ones reflections. However, *Moral Intelligence* in practice is reinforced by voluntary tasks, such as the Global Compact or Corporate Governance, as well as by the law. Often there is an apparent difference between the lived rules and the corporate norms (a company's morality).

Moreover, as the article of Bardy and Rubens shows, there are variations between business ethics and the models of Corporate Governance in the U.S. and continental Europe. Notwithstanding the differences, they conclude that in order to solve ethical issues it needs a rational theoretical (even philosophical) foundation on the one hand and a specific content that is generated from real-life experiences on the other hand.

While the methodical reflection on morality is another category, namely business ethics, than morality itself, it is of utmost importance that the ethical knowledge of intellectuals and of a critical public does not persist in a purely theoretical discussion, but that they seek a dialogue with practical economy.

However, it is hard to breach the economic logic, especially in large corporations. The compulsion to satisfy the *shareholder value* on the management level is carried forward throughout the whole corporate hierarchy by given objectives and performance-based salaries. Meanwhile, a practical economy that strives to meet ethical demands, needs managers who behave in a way that they can be taken as role models.

The difficulties of implementing some sort of *Moral Intelligence* in IT-projects are shown by the experiences of Manders-Huits and Zimmer in two different technical design communities: Vehicle Safety Communication Technology and User Profiling Infrastructures. Their attempts to influence the design of technologies revealed "discouraging results" and lead them to define three "Key Challenges of Value-Conscious Design" in order to overcome crucial pragmatic challenges in future projects.

When it comes to *Business Intelligence* meeting *Moral Intelligence*, the media plays a decisive role in that it filters overall information and frames the set of values. Scrutinising the value judgements of the media with regard to the content as well as to the methodology could lead to a more objective and balanced view of those frictions that become apparent in talk shows, newspapers and Internet forums.

It is noteworthy that due to developmental progress within communication technologies 'the civil society catches up'. The Internet has deregulated the media by depriving its power. Hence the *citizen* has more possibilities of participation in society now, more than ever. Yet this opportunity faces the risk that the data obtained by *Business*

Intelligence is misemployed like with new forms of corporate espionage, a higher vulnerability of business secrets, the balance between corporate privacy and publication as well as the modified relation to one's own privacy within social Internet portals.

Spence, who is topping off the issue at hand, is concerned with the media whose "'business intelligence' must be congruent with 'moral intelligence'", while in conflict situations the moral aspect always has priority. Furthermore, Spence accentuates the responsibility of the media that produce and distribute a good that is public just like food and medicine: information, which is according to the author "*doubly normative*".

This issue aims at inspiring a further and more detailed research in *Business* and *Moral Intelligence*. Only a few aspects of this rather new and roughly defined field are touched here and it must remain less than a general overview. Still we hope to give the reader an idea of this manifold matter that will gain in importance with the further development of technology.

Yours sincerely,

Yvonne Thorhauer and Stefan Blachfellner,

The Editors

Albrecht Fritzsche:

The simulated traces of action - B.I. and reflection through technology

Abstract:

Business Intelligence can be interpreted as a compensation for the growing complexity of technical support in economic transactions. With the help of sophisticated calculation and analysis tools, the business situation is simplified for the user in order to enable reasonable decisions. However, the simplicity of Business Intelligence is only simulated by hiding the system operations under the surface. This causes a disruption of the general concept of reasonable action. The notion of responsibility disappears between the business expert and the systems engineer. A possible solution to this problem is to change the system design process and to introduce competing technology which could show new traces of the system operation.

Agenda

An ethical challenge	4
Ubiquity and intransparency.....	4
Decision making and orientation	4
Technology and reflection.....	5
The loss of traces.....	6
The simulated traces	6
IT experts, users and morality.....	7
The pragmatism of provisional ethics.....	7
Business experts and system engineers	8

Author:

Albrecht Fritzsche:

- Organization and contact address: Universität Stuttgart, Institut für Philosophie, 70174 Stuttgart, Germany
- Telephone, email and personal homepage: ✉ almamarf@gmx.net
- Relevant publications:
 - Engineering Determinacy - The exclusiveness of technology and the presence of the indeterminate. WPE 2008 proceedings, to appear 2009.
 - Wo die Technik den Menschen verbirgt, to appear 2009.

An ethical challenge

Business Intelligence has lately become a very popular term in information technology. As it happens with popular terms, a variety of different applications are subsumed within BI. In a broad sense, every kind of tool that processes economic information can be called Business Intelligence: data extraction, transformation and loading procedures in a data warehouse, data marts, data mining tools, planning and optimization systems. In a specific sense, Business Intelligence is narrowed down to Online Analytical Processing (OLAP), Management or Executive Information Systems (MIS / EIS) and special front-ends with sophisticated reporting and planning functionality¹. Being called Business Intelligence, all such technology should show a common characteristic. Since its technical design is quite diverse, this characteristic can only be found in the field of application: Business Intelligence is used to support business decisions. In other words: BI describes a certain activity, not a certain technology. It would not have been necessary to coin a new term just to describe how the computer systems mentioned above work and what can be done with them. Business Intelligence marks a change of perspective to their application: IT is now considered as an essential element of the process of decision making itself. With Business Intelligence, we are not only able to decide better or more efficiently. We are able to decide in a completely new way, sharing the authority for our decisions with the technology we use. Where this happens, the usage of IT creates an ethical challenge.

Ubiquity and intransparency

The last two decades have brought a major change to the role of IT in business practice². Before that time, access to the information necessary for sound business decisions had been rather limited. The storage and the exchange of business data were slow, poorly coordinated and costly. Limited data availability was a severe restriction on the possibilities of how and where to do business. With the introduction of powerful computer systems, data

warehouses and communication networks, this problem disappeared. It became possible to store and transmit any commercial information that appeared in a business transaction. Similar data from different sources could be amalgamated, consolidated and aggregated; complex interactions between business processes could be identified, analysed and managed. Without this progress in IT, the recent growth of international markets, outsourcing, globalisation and worldwide supply and production networks would hardly have been possible.

However, this development had an important side effect: All business processes were penetrated by technical applications. As much as IT has enabled economic growth, it has become an irreplaceable part of it. Distributed production facilities, off-shore services, electronic payment, individual consumer response and network management all depend on the availability of information technology. Without electronic data processing, business as it is performed today would not only be slowed down or have a lower level of efficiency; it would be impossible. In today's world, IT is present everywhere and its contribution to our actions is so sophisticated that we hardly even realize it³.

Decision making and orientation

Limited information has an important advantage: decisions are much easier. With a growing number of interrelated variables and data instances, it becomes increasingly hard to understand what consequences a decision might have⁴. Modern distribution and supply networks, for example, have often reached a complexity where sophisticated products assembled with parts from dozens of different suppliers are produced for other dozens of different markets. The automotive industry had a leading role in this development: in recent years, the number of car models has more than tripled, various additional features for safety and comfort have become standard in modern automobiles and many new markets have emerged which require

¹ See Gluchowski, P. et al.: Management Support Systeme und Business Intelligence or Michalewicz, Z. et. al.: Adaptive Business Intelligence.

² See e.g. Kamper, H.-G. et al.: Business Intelligence – Grundlagen und praktische Anwendungen.

³ Gamm, G.: Technik als Medium, pp102; Hubig, Ch.: Die Kunst des Möglichen I, pp186.

⁴ See English T. M.: Optimization Is Easy and Learning Is Hard in the Typical Function or Cantermann A.: Handeln in komplexen Zusammenhängen.

special attention⁵. Under these circumstances, it is generally impossible to find optimal solutions to a decision problem with analytic methods of conclusion. Many companies have therefore introduced advanced planning systems which achieve good solutions in an acceptable time frame, but at the price of missing formal representation. Determinate analytical conclusions become impossible. The decision maker can justify the solutions only by the fact that nothing better can be found⁶.

The users of huge data warehouses have to face a problem which looks in many ways rather similar. A large amount of data from various sources, generated in different ways, has been adapted, consolidated and transformed within the warehouse. Each set of data can undergo hundreds of different routines during which it can be rejected, replaced and/or changed. The end result of these routines cannot be verified by the user. Data mining tools and other analysis methods add further procedures for pattern recognition and pre-selection of data volumes. Data processing with such tools does not necessarily cause errors. In fact, the tools will usually offer the most – if not the only – accurate way available to treat the data. However, for the very reason that they enable work that would otherwise not be possible, they also change the meaning of technology: The most defining aspect of it, its determinacy, disappears.

Technology and reflection

It has recently become popular to consider technology as an essential aspect of the human being in the world. In this sense, technology is "humanity at work"⁷; technology is the general mode of human action⁸. Much of these ideas can be traced back to Friedrich Hegel and the image of human action becoming external. With technology, an action is executed at a distance from the actor, which makes

it possible to control it and reflect upon it⁹. In fact, it seems that reflection in general needs an external point of view. If this is true, the distance to one's own actions is in fact an indispensable aspect of establishing oneself as an actor at all. The determinate structures of cause and effect in technical operations provide such a distance. Technology therefore shapes our thinking in general. It is, as Christoph Hubig puts it, a term of reflection¹⁰.

While technical determinacy thus seems necessary to reflect on action, reflection itself is necessary because of the indeterminacy of action. Inasmuch as an action intends to change one state of the world into another, its technical expression will always remain incomplete. Whatever happens in the course of the action will exceed technical description. Most of the time, the result and the intention of the action will not be identical. It was also Hegel who pointed out that the difference between the two is actually essential for human reason¹¹. If there were no difference, the actor would not be able to distinguish between him/herself as the master of the action and the application of technology as its execution: If the means always achieved the end, no distinction between the two would be possible.

From a mere technical perspective, it is enough to consider the user in as far as he/she has an impact on the operation of the machine. In case of Business Intelligence, this means that the user is the source of the information that initiates and controls the course of the following calculations. There is no inherent need in technical thinking to give the user insight into the execution, because everything that happens has already been determined by the input. Whether the result of the calculation is displayed to the user, to another person, or whether it disappears without a trace does not matter for technology. However, considering what has been said above, it matters quite a lot for human action. Without traces, it is impossible for the user to tell the difference between the intended effect and the actual outcome.

⁵ Recent figures in VDA: Auto-Jahresbericht 2007 and ISI: Deutscher Delphi-Bericht zur Entwicklung von Wissenschaft und Technik

⁶ See Meyer C. M.: Integration des Komplexitätsmanagements in den strategischen Führungsprozess der Logistik and Gerberich C. W.: Managen der Komplexität und Dynamik.

⁷ Pitt, J.: Thinking about Technology, p11.

⁸ Fischer, P.: Philosophie der Technik, pp32.

⁹ Hegel, G.W.F.: Phänomenologie d. Geistes, pp140.

¹⁰ Hubig, Ch.: Die Kunst des Möglichen I, p230.

¹¹ Hegel, G.W.F.: Phänomenologie d. Geistes, pp294.

The loss of traces

With Christoph Hubig, we can describe this problem in today's technology as a loss of traces¹². The permanent presence of complex and interactive technical applications in our life makes it increasingly hard to distinguish determinate technical procedures from their environment. Separate effects cannot be associated to separate operations. As a consequence, the authority of the user over the application of technology vanishes. We cannot distinguish our objectives as a user from the operation of technology any more. Instead of saying that we work with technology, we can now only say that we initiate it or and run it. This would not be such a problem if technology were complete – if it covered the user's complete view of the world. But in reality, most of the background of a given situation will remain implicit to the application of the technology. All input to a calculation will always be an approximation, not only because of time and storage space, but also, because explicitness can only be achieved by the very means of technology itself.

Taking a closer look, the simplest numeric data that are input into technical systems convey some sort of approximation. Putting daily sales figures into a data warehouse, for example, seems to be a quite straightforward activity, but even here, space is left for interpretation e.g. whether a sale refers to a verbal agreement, a signed contract or a transfer of goods. The description of the customer, the product itself, or the point of sale might give cause for additional questions. In a direct conversation, one might sooner or later understand in general what information is expected. In front of a computer screen, this remains unclear. Nobody knows who will use the data and to what end, and at the other side of the system, background details concerning the data input remain invisible, too.

Similarly, the preferences put into a search system might be honest expressions of what the user thinks at that moment, but quite certainly there will be further, implicit understandings that these preferences only hold within certain boundaries and that some features in the search space will take precedence over others in case of a conflict. The user might not even know all this. If he/she were searching on his/her own, this would hardly matter, but in this case, the system executes the search. Seeing the result, the user cannot tell how many of his/hers

implicit understandings have been complied with or where the search would have ended with just slightly different preferences.

The simulated traces

Where the concepts of action dissolve in the size and complexity of technical operations, the only way to restore human authority over systems is simplification. Ubiquitous and intransparent technology that has become indeterminate has to be broken down into separate pieces over which the users re-establish their authority. Such a deconstruction, however, would severely diminish the benefit of technology. In fact, most of the efficiency that the latest technical developments achieve seems to be gained as a trade-off against human control.¹³ For a society whose economy is based on constant expansion, this would cause a fundamental contradiction. Business Intelligence therefore provides another solution.

Online Analytical Processing of the information in a data warehouse allows the user to navigate more easily through huge data volumes, to aggregate data and condense them into variable, simple reports. Routines of automatic data consolidation and adaptation in the initial phase enhance the quality of user input and smooth out mistakes and contradictions. Management Information Systems use optimized graphical data presentation and standard reporting layouts (e.g. the famous balanced scorecards) to point out the most significant issues for business decisions. Context sensitive search routines and forecasting by simulation introduce replacements for the general knowledge of its users inside the systems. In order to support human decisions, Business Intelligence thus hides in many different ways the size and complexity of technology behind simplified interfaces. In other words: Business Intelligence does not restore authority over the original technical operations – it compensates for their disappearance with the introduction of new environments of action on top of the technology. With Business Intelligence, it becomes possible to work on the focal points that are provided to the users. Pressure can be put on the areas with critical performance figures; preferences for planning can

¹² Hubig, Ch.: »Wirkliche Virtualität«, pp53.

¹³ See also Wiegerling, K.: Philosophische Aspekte der Mensch-Technik-Interaktion. Whether or not some technical artefacts have to be treated like autonomous actors, as e.g. in ANT, is not to be discussed here.

be setup in a more sophisticated way. And the systems do present traces of the action with the change of the figures and the simulation of planning results. However, these traces are not the traces of the underlying technology, but only their simulation at the surface where the Business Intelligence is installed.

IT experts, users and morality

The typical data warehouse has at least three different layers of data, one for input, one for transformation and one for output. Additional layers for input control, logging and output consolidation are becoming more and more popular. Business Intelligence with OLAP and MIS is restricted to the data in the output layer, automatic routines to the transformation layer. Whatever happens before remains outside the scope. Systems for advanced planning, forecasting and simulations make it easier to express preferences for the calculations and to check the results, but they do not affect the procedures of the calculation themselves. Considering this, it becomes clear that the problem of authority over the action is not solved with Business Intelligence; it just shifts it elsewhere. The critical point is not the usage of the system any more but its implementation. The user does not have to bother about dealing with technology any more, because everything has become easy. Instead, the systems engineer now carries full responsibility for ensuring that the system gets simplified correctly.

The typical company structure sets departments for information technology apart from business units. In addition, most projects for the implementation of Business Intelligence are run by external experts. Even if these experts have a professional training in economy, they lack the specific competence and experience to take responsibility for the business transactions of the company. This duty falls on the business unit. But in case of Business Intelligence, the user's decisions are interconnected with the design of the system. What the user thinks is right depends on the consolidation procedures, aggregation methods, search routines and presentation techniques implemented in the system. At the same time, the only person able to build and change the system and to tune its performance parameters is the IT expert.

The pragmatism of provisional ethics

Considering the loss of traces in today's technology, Christoph Hubig suggests a new pragmatism to

sharpen the terms of our decisions with respect to the practical relevance they might have for our actions¹⁴: we should use our freedom of choice to establish those concepts of action that seem necessary to us in the world. As soon as they are clarified, we have to shape our technology accordingly to confirm them. This is to be achieved by the intentional setting up of boundaries for technical applications. First, the range to which technology penetrates our life should be limited. Second, a possibility to establish transparency in the system should be available "on demand": According to the Stuttgart concept of Parallel communication, fractions should be introduced in the permanent flow of technology wherever it is necessary to assure access to determinate operations.¹⁵

Applied to Business Intelligence, this could mean that the course of system development has to be inverted. Instead of additional systems, which are added on top of an existing architecture, the design of the applications for Business Intelligence should take precedence. BI should not make sense of the data available; it should make data available in a sensible way. As a consequence, the engineer should follow the lead of the business experts and at the same time require their participation in all further endeavours to improve and expand the technical architecture. Many common approaches to software development, e.g. requirements engineering, already incorporate these suggestions¹⁶. In other cases, e.g. rapid prototyping, it is represented as a feedback circle spanning over the complete range of the engineering project. However, the application of these methods is often incomplete. It stops before the underlying complexity of data warehouses, search algorithms etc. is addressed.

It still remains unclear in what way fractions in the permanent flow of technical operations can be introduced, because they appear as mere obstructions to efficiency. One solution might be the introduction of competing technology. Fractions then are differences between separate systems. While these differences may not resemble the traces that a technical operation leaves in a given reality, they still allow reflection on the effectiveness of the technology, which can lead to the desired separation

¹⁴ Hubig, Ch.: »Wirkliche Virtualität«, 60.

¹⁵ Wiegerling, K: Das Grundproblem des UbiComp und das Stuttgarter Konzept der Parallelkommunikation.

¹⁶ Hood, C. et al: Requirements Management, pp10.

of means and ends. The traces of action still remain simulated, but they appear now between separate technical applications and not within a single one.

Business experts and system engineers

Ubiquitous, intransparent IT challenges rational decision making and acting, because the traces of the action in the real world disappear. Without these traces, technology loses its determinate quality. As a consequence, it becomes difficult to assign responsibilities in the usage of IT. Economic decision makers are greatly affected by this problem, because they work with complex and dynamic IT systems and huge amounts of data. In many situations, decisions are made under circumstances which do not allow their reflection according to their outcome. Technology then loses its status as a separate determinate instance between the actor and the world.

BI systems can be understood as a compensation for this problem. They restore the possibility for their users to decide and act rationally. In order to achieve that, they simplify the decision making situation at the front-end by excluding the complexity of the preceding layers of technology. For the user of these systems, it seems as if all the insoluble complexity issues have disappeared. However, they have just been shifted to the systems engineer. The engineer is concerned with technical efficiency, but the implications of the content of the system for business decisions will remain largely unclear. As a consequence, neither the business expert nor the engineer has the necessary insight to take responsibility for the decisions to be made with the system. In such a situation, moral behaviour seems practically impossible. Hubig's concept of provisional ethics implies that a solution might be given by the inversion of the course of system design and the pluralism of technical applications. In this way the authority of the user of Business Intelligence over his/her actions might be able to be restored.

References

- Cantermann A.: *Handeln in komplexen Zusammenhängen*. In: Sommerlatte T 2002 (ed.): *Angewandte Systemforschung*, Wiesbaden 2002, 68-79.
- English T. M.: *Optimization Is Easy and Learning Is Hard in the Typical Function*, *Proceedings of the 2000 Congress on Evolutionary Computation: CEC00*, 924-931.
- Gamm, G.: *Technik als Medium. Grundlinien einer Philosophie der Technik*. In: Hauskeller M et al. *Naturerkenntnis und Natursein*. Frankfurt a M. 1998, 94-106.
- Gerberich C. W.: *Managen der Komplexität und Dynamik*. In: Maier F (ed.): *Komplexität und Dynamik als Herausforderung für das Management*. Wiesbaden 2004. 235-259.
- Gluchowski, P. et al.: *Management Support Systeme und Business Intelligence*. Berlin 2008²
- Fischer, P.: *Philosophie der Technik*, Munich 2004.
- Hegel, G.W.F.: *Phänomenologie des Geistes*. Bamberg, Würzburg 1807. Reprint Stuttgart 1987.
- Hood, C et al.: *Requirements Management: Interface Between Requirements Development and All Other Engineering Processes*. Berlin 2007
- Hubig, Ch.: *Die Kunst des Möglichen I. Technikphilosophie als Reflexion der Medialität*. Bielefeld 2006.
- Hubig, Ch.: »Wirkliche Virtualität« Medialitätsveränderung und der Verlust der Spuren. In: Gamm G, Hetzel A: *Unbestimmtheitssignaturen der Technik*. Bielefeld 2005, 39-62.
- ISI (Fraunhofer Institut für Systemtechnik und Innovationsforschung): *Deutscher Delphi-Bericht zur Entwicklung von Wissenschaft und Technik*, Bonn 1993.
- Kamper, H.-G. et al.: *Business Intelligence – Grundlagen und praktische Anwendungen*. Wiesbaden 2004.
- Meyer C. M.: *Integration des Komplexitätsmanagements in den strategischen Führungsprozess der Logistik*. Bern u.a. 2001.
- Michalewicz, Z. et. al.: *Adaptive Business Intelligence*. Berlin 2007.
- Pitt, J.: *Thinking about Technology*. New York 2000.
- VDA: *Auto-Jahresbericht 2007*. Frankfurt 2007.
- Wiegerling, K.: *Philosophische Aspekte der Mensch-Technik-Interaktion beim Ubiquitous Computing*. *Concordia* 53, Januar 2008. pp39-63.
- Wiegerling, K.: *Das Grundproblem des UbiComp und das Stuttgarter Konzept der Parallelkommunikation*. In: GI (ed.): *Informatik trifft Logistik. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e.V. Proceedings 110/2*, Bonn 2007. pp359-363.

Oliver Siemoneit:

Business Intelligence and Ambient Intelligence - Some thoughts on the main trends of business information processing, their opportunities, problems and limitations.

Abstract:

Ambient Intelligence, often also referred to as Pervasive Computing, Ubiquitous Computing or Context-Aware Computing, is supposed to have a lot of advantages for future business information processing. However, as in many cases, technological developments do not only provide opportunities, improve work conditions and make life more comfort for customers, but they also give rise to new problems. Aim of this paper is to discuss the pros and cons of Ambient Intelligence for future business intelligence on the basis of two scenarios. The first scenario deals with next generation manufacturing, the so-called smart factory. The second scenario is about different concepts of actuarial fairness based on Ambient Intelligence technology in the insurance industry, mainly different pay-as-you-drive-solutions. The infringement upon privacy is identified as main problem in both scenarios. Besides an in-depth discussion on this which opens up a much broader view on Ambient Intelligence in future business intelligence, different technical solutions are to be roughly outlined that could help to avoid some crucial problems.

Agenda

Problemstellung, Zielsetzung, Vorgehensweise..... **Fehler! Textmarke nicht definiert.**

Fallbeispiel 1: Intraorganisationale Effekte der Ambient Intelligence am Beispiel der Smart Factory**Fehler! Textmarke nicht definiert.**

Fallbeispiel 2: Extraorganisationale Effekte der Ambient Intelligence am Beispiel des Pay-As-You-Drive **Fehler! Textmarke nicht definiert.**

Zusammenfassung und Ausblick **Fehler! Textmarke nicht definiert.**

Author:

Dipl.-Kfm. techn. Oliver Siemoneit:

- Organization and contact address: Institut für Philosophie, Universität Stuttgart, Seidenstrasse 36, D-70174 Stuttgart, Germany
- Telephone, email and personal homepage: ☎ +49 - 711 - 685 82491, ✉ oliver.siemoneit@philo.uni-stuttgart.de

Problemstellung, Zielsetzung, Vorgehensweise

Der rasante Fortschritt im Bereich der Nanotechnik, der Mikrosystem- und Kommunikationstechnik hat in den letzten Jahren eine modifizierte Art und Weise des Einsatzes klassischer Informations- und Kommunikationssysteme mit sich gebracht. Unter den Stichworten Context-Aware Computing, Pervasive Computing, Ubiquitous Computing und Ambient Intelligence wird dies in letzter Zeit auch häufig diskutiert (vgl. exemplarisch Phillips/Wiegerling 2007 und die dort angegebene Literatur). Ambient Intelligence ist dabei keine neue Technik, sondern die Vision einer veränderten, zukünftigen Anwendungsform herkömmlicher Informations- und Kommunikationssysteme, die durch Miniaturisierung und Einbettung in Objekte des täglichen Gebrauchs sowie durch drahtlose Vernetzung und Allgegenwart im Alltag gekennzeichnet ist (Siemoneit et al. 2005).

Ziel des vorliegenden Beitrags ist es, eingehend die Auswirkungen der Ambient Intelligence auf die Business Intelligence zu diskutieren, die Möglichkeiten, Probleme und Grenzen des Einsatzes dieser Techniken aufzuzeigen bzw. technische Lösungen zu präsentieren, bei denen aus technikethischer Perspektive auch von einer akzeptablen, gerechtfertigten Lösung gesprochen werden kann. Diese Diskussion erfolgt exemplarisch anhand zweier Betrachtungsgebiete: Fallbeispiel 1 untersucht aus einer intraorganisationalen Perspektive heraus, wie Ambient Intelligence unternehmensinterne Prozesse und Abläufe verändert und welche Potentiale sowie Herausforderungen hierbei erwachsen; Fallbeispiel 2 geht aus einer extraorganisationalen Perspektive darauf ein, wie sich die Wertschöpfungsprozesse hin zum Kunden verändern.

Fallbeispiel 1: Intraorganisationale Effekte der Ambient Intelligence am Beispiel der Smart Factory

Im Gegensatz zur Konsumgüterindustrie, in der eine Großserienfertigung mit standardisierten Komponenten vorherrscht, ist der Investitionsgüterindustrie geprägt von Einzel- und Kleinserienfertigung, maßgeschneiderten Kundenlösungen bei geringer Losgröße und großer Variantenzahl. Der hohe Individualisierungsgrad der Produkte erfordert, dass bei der Produktion eine Vielzahl hochspezialisierter, für einzelne Bearbeitungsaufgaben angepasste Werk-

zeuge und Vorrichtungen zum Einsatz kommen. Die Betriebsmittelverwaltung und -logistik nehmen unter diesen Bedingungen oft schwer handhabbare Formen an. Die umfassende Proliferation bzw. Einbettung kleinster Informations- und Kommunikationssysteme in Betriebsmittel soll die Fabrik der Zukunft „smart“ bzw. „intelligent“ machen und dazu beitragen, diese Komplexität besser zu beherrschen (Siemoneit/Jendoubi/Bauer 2004, Jendoubi 2007). Ziel ist die Schaffung von Transparenz (z.B. über Ort, Zustand/Verschleißgrad von Betriebsmitteln), die Vereinfachung von Prozessen durch Automatisierung und teilautonomes Verhalten bzw. die Verbesserung der Betriebsmittellogistik („Das richtige Werkzeug, zur richtigen Zeit am richtigen Ort“). Die umfassende Erfassung von Maschinendaten und Prozesskennzahlen in Echtzeit ermöglicht zudem eine exakte Analyse von Fehlern und Ineffizienzen, die zeitnahe Kontrolle, Steuerung und Planung von Produktionsabläufen und damit ein umfassendes Produktionscontrolling und Produktionsmanagement.

Der Einsatz von Ambient-Intelligence-Technologien in der Fertigung bringt eine Vielzahl von Vorteilen mit sich. Neuartige technologische Entwicklungen schaffen jedoch immer zugleich auch neue Problemlagen bzw. verschärfen existierende Problemlagen in eine Richtung, die der eingehenden Erörterung bedürfen. So beginnt die Vision der smarten, intelligenten Fabrik etwa dort problematisch zu werden, wo der Mensch in den Informationssystemen nur als ein optimierungsbedürftiger Parameter bzw. als Ressource neben vielen anderen in Erscheinung tritt: Unter planerischen Gesichtspunkten scheint kaum mehr ein Unterschied zu bestehen zwischen einem mit RFID-getaggtten Werkstück und einem per Lokalisationssystem ortbaren Mitarbeiter. Beide müssen in effektiver und effizienter Weise eingesetzt und „verwandt“ werden, um die Produktionsmaschinerie optimal am Laufen zu halten. Der Mensch gerät hier zunehmend unter die Herrschaft der Systeme, die er sich einst selbst geschaffen hat, welche nun aber beginnen, in einer Eigenlogik den Menschen selbst zu beherrschen. Es sind die Systeme, die zunehmend für uns entscheiden und uns in optimaler Weise einsetzen und nicht wir, die aufgrund von Systemempfehlungen Entscheidungsunterstützung erhalten (Siemoneit et al. 2005 S. 173ff.).

Aber auch bei einem recht verstandenen Einsatz von Lokalisationstechniken und Ambient-Intelligence-Lösungen in der Fertigung entstehen weitere tiefgreifende Probleme: Es ist dies vorwiegend das Problem der Privatheit am Arbeitsplatz. Ambient-

Oliver Siemoneit:

Business Intelligence and Ambient Intelligence - Some thoughts on the main trends of business information processing, their opportunities, problems and limitations.

Intelligence-Lösungen erlauben die detaillierte Erfassung einer Vielzahl personenbeziehbarer Daten, die die Erstellung fein-granularer Bewegungsprofile von Mitarbeitern, die exakte Erfassung von Bearbeitungs-, Pausen- und Leerzeiten bzw. eine genaue Zurechenbarkeit von Fehler bei Produktionsabläufen ermöglichen. Zwar hat ein Arbeitgeber das Recht, die Erfüllung von Aufgaben und Rollenverantwortungen seiner Mitarbeiter zu kontrollieren. Die Intensität bzw. Art und Weise hat jedoch Grenzen: Der Arbeitnehmer verkauft ja schließlich nicht sich, sondern seine Arbeitskraft (Persson/Hansson 2003 S. 63f.). Die eingesetzten Kontrollmaßnahmen müssen deshalb adäquat und angemessen sein bzw. so datensparsam und minimal-invasiv wie möglich erfolgen. Der Arbeitnehmer ist vor überbordenden Kontrollmaßnahmen zu schützen ebenso wie vor überzogenen Erwartungen an die Leistungserfüllung. Der Verkauf der eigenen Arbeitskraft impliziert zwar die Notwendigkeit, eine gewisse Arbeitsleistung zu erfüllen, sicherlich jedoch nicht immer das absolute, persönliche Maximum (oder sogar noch ein bisschen mehr), das den Mitarbeiter täglich an bzw. über die individuelle Erschöpfungsgrenze bringt (Persson/Hansson 2003 S. 65). D.h.: Der Arbeitnehmer hat auf der einen Seite das Recht auf Privatheit am Arbeitsplatz bzw. auf einen geschützten, persönlichen, intimen Raum. Diesem Schutzraum stehen jedoch auf der anderen Seite legitime Interessen und notwendige Pflichten des Arbeitgebers konfligierend gegenüber (Kontrolle der Aufgabenerfüllung, Arbeitsschutzmaßnahmen, Schutz Dritter etc.), wobei es gilt, beide Interessenlagen – sowohl die des Arbeitnehmers als auch des Arbeitgebers – deziert und im Einzelfall gegeneinander abzuwägen. Privatheit – auch am Arbeitsplatz –, das sollten die vorangegangenen Ausführungen deutlich gemacht haben, ist jedoch ein Wert an sich, der in liberal-demokratische Gesellschaften einen grundlegenden, konstitutiven Stellenwert hat und den es daher zu schützen gilt (Rössler 2001, Heesen/Siemoneit 2007).

Ein technischer Lösungsansatz zum Schutz der Privatheit in intelligenten Fertigungsumgebungen von morgen besteht darin, den Mitarbeiter aus dem Netz mobiler, kommunizierender, smarter Betriebsmittel herauszunehmen (ihn also nicht zu einem optimierungsbedürftigen Ding zu machen) bzw. statt Lokalisations- und Trackingtechniken diverse Ansätze der situationsadäquaten Selbstpositionierung zu verwenden (vgl. ausführlich Siemoneit et al. 2008). Eine Bildung detaillierter Bewegungsprofile wird somit verunmöglicht bzw. erschwert, nichtsdestotrotz ist der Fabrikarbeiter von den vielen Vorteilen

der Ambient Intelligence – etwa der kontextabhängigen Bereitstellung und Präsentation benötigter Informationen – nicht vollständig abgeschnitten.

Fallbeispiel 2: Extraorganisationale Effekte der Ambient Intelligence am Beispiel des Pay-As-You-Drive

Auch im extraorganisationalen Bereich besteht der wesentliche Beitrag der Ambient Intelligence darin, qua Einbettung von Informations- und Kommunikationssystemen in Alltagsgegenstände die Bereitstellung bisher nicht erfasst bzw. erfassbarer Daten in Echtzeit in die Systeme der betrieblichen Business Intelligence zu ermöglichen. Die reale Welt soll in die digitale Welt automatisch „abgebildet“ werden – so die häufig zu findende Rede. Die zeitaufwendige und oft fehlerhafte Eingabe der Daten per Hand soll entfallen und den Weg frei machen für weitere Optimierungen betriebsinterner Prozesse und Abläufe, einen engeren intensiven Kontakt zum Kunden, ein Closed-Loop- und One-To-One-Marketing (Mattern 2003, Fleisch/Mattern 2005).

Vor allem einige Versicherungsunternehmen haben in letzter Zeit das Pay-As-You-Drive – eine personalisierte, nutzenabhängige und risikoadjustierte Kraftfahrzeugversicherungspolice auf Basis von Ambient-Intelligence-Lösungen – für sich entdeckt, um sich gegenüber Konkurrenten erfolgreich zu differenzieren und den Kontakt mit dem Kunden zu intensivieren (Oberholzer 2003, Filipova/Welzel 2005, Filipova 2007). Fahrstrecke (Haupt- oder Nebenstraßen? Innenstadt bzw. Überland?), Fahrzeit, Witterungsverhältnisse, Telemetriedaten (Anfahr- und Abbremsverhalten, Abstand zum Vordermann, Blinkerbenutzung etc.) werden von einer On-Board-Unit bzw. Black Box im Fahrzeug registriert und an das Versicherungsunternehmen weitergeleitet, das dann aus den gewonnenen Daten eine individuelle Risikoprämie kalkuliert, die der Versicherungsnehmer zu entrichten hat. Die „guten“, vorsichtigen Fahrer werden durch eine niedrige Prämie belohnt, die „schlechten“, riskanten Hasardeure und Raser für ihr Fahrverhalten bestraft, weil jeder gemäß seines persönlichen Risikoprofils punktgenau tarifiert wird (Konzept der sog. „Actuarial Fairness“). Ökonomisch gesprochen ermöglicht die genannte Ambient-Intelligence-Lösung damit eine weitreichende Reduktion von Informationsasymmetrien zugunsten des Versicherungsunternehmens und verhindert – zumindest in der ökonomischen Mo-

dellwelt idealer, vollkommener Märkte und des vollständig rationalen Homo Oeconomicus – ein Marktversagen durch Adverse Selection (vgl. dazu ausführlich Filipova/Welzel 2005, Filipova 2007 bzw. kritisch dazu Horsch 2005).

Auf den ersten flüchtigen Blick scheint aus ethischer Perspektive nichts gegen ein Pay-As-You-Drive zu sprechen: Umsichtiges Fahren, das andere Verkehrsteilnehmer schützt, wird belohnt, unverantwortliches Fahren sanktioniert, indem Prämien verteuert werden bzw. der Versicherungsschutz gänzlich versagt wird. Betrachtet man aber Mobilität als eine Art verbrieftes Grundrecht, das für jeden Bürger liberal-demokratisch verfasster Gesellschaften zu einem erschwinglichen Preis zu haben sein sollte, wird die Problemlage schon schwieriger: Gerade junge Fahrer (Fahranfänger) als auch ältere Fahrer (Rentner) müssen (jetzt schon) oft erheblich höhere Prämien entrichten, weil sie als risikobehafteter gelten als der Durchschnitt. Aus ethischer Perspektive als besonders problematisch erweist sich der Einsatz von Ambient-Intelligence-Lösungen im Versicherungsgeschäft dann, wenn man bedenkt, dass die Idee der risikoindividuellen Tarifierung nicht nur auf das sog. Nicht-Leben-Geschäft begrenzt ist, sondern auch auf das Leben-Geschäft (etwa Lebens- und Krankenversicherungen) übertragen werden kann:

„Adidas could offer, manage, control individualized training programs based on the data acquired from communicating sensors in Adidas sport shoes. This information could be used by the health insurance company and prices would be adapted according to the training efforts of an insurance holder. One step further Adidas could offer new insurance products itself as an intermediary“ (Müller/Zimmermann 2003 S. 7).

Gerade jedoch im Gesundheitssektor sind dem Konzept der „Actuarial Fairness“ enge Grenzen gesetzt: Der Versicherungsnehmer hat hier oft nicht die volle Entscheidungsfreiheit bzw. Wahl hinsichtlich seiner gesundheitlichen Veranlagungen und Dispositionen. Das Konzept der „Actuarial Fairness“ würde hier die von Natur aus gesundheitlich besser Gestellten bevorteilen und die schlechter Gestellten benachteiligen, indem ihnen die volle Bürde ihres Schicksals auferlegt wird. Die schlechter Gestellten würden damit aber für etwas verantwortlich gemacht werden, wofür sie gar nicht verantwortlich gemacht werden können. Dies ist aus ethischer Perspektive kaum rechtfertigbar, handelt es sich doch um einen Sachverhalt, der in Widerspruch

treten kann zu dem basalen Recht auf ein menschenwürdiges Leben bzw. dem Recht auf Selbstentfaltung.

Das Hauptproblem von Ambient-Intelligence-Lösungen im extraorganisationalen Bereich hin zu Kunden ist aber, dass hier große Mengen sehr persönlicher Daten erhoben werden, die genaue Rückschlüsse auf Freizeitverhalten, Präferenzen und Aktivitäten erlauben – also Daten, die in dieser Fülle und diesem Detailgrad kaum in die Hände von Unternehmen gelangen sollten. Seit Jahren beobachten Datenschützer daher mit Sorge den Trend zu immer umfangreicheren Datensammlungen und Datenverbünden in der Privatwirtschaft (Siemoneit et al. 2005 S. 213f.). Das legitime Interesse der Wirtschaft, möglichst viel über den Kunden zu wissen, um seine ungestillten Bedürfnisse zu erfahren und möglichst profitabel zu befriedigen bzw. das legitime Interesse der Wirtschaft am Schutz vor zahlungsunwilligen Kunden und Betrügnern ist zwar verständlich, die Gefahr besteht jedoch darin, dass einzelne Datenbestände zusammengeschaltet werden und der Kunden somit „gläsern“ wird und – bei Nichterfüllung gewisser Kriterien – automatisch und kaum revidierbar als nicht vertrauenswürdig, zahlungsunwillig, insolvent etc. stigmatisiert wird. Umfassende Datensammlungen in der Privatwirtschaft bergen aber auch immer das Potential des Missbrauchs. Gerade die Skandale um die Telekom AG im Jahr 2008 haben die Probleme und Gefahrenlagen umfassender Datenbestände und Datenverbünde weiten Bevölkerungsteilen erstmals deutlich vor Augen geführt: Missbräuchliche Auswertung/Verwendung von Verbindungsdaten, der Verlust sensibler Kundendaten (Anschrift, Bankverbindung, nicht-öffentliche Telefonnummern etc.) bzw. der Verkauf von Kundendaten an Dritte etwa zur Bonitätsbewertung (vgl. exemplarisch Lessmann 2008, Murphy 2008).

Aus datenschutzrechtlicher bzw. ethischer Perspektive ist es daher wünschenswert, Ambient-Intelligence-Lösungen im Business-To-Consumer-Bereich von vorne herein möglichst datensparsam zu konzipieren, denn Datenvermeidung ist immer noch der beste Datenschutz. Dies ist auch technisch ohne weiteres möglich: Eine ethisch gerechtfertigte bzw. gut rechtfertigbare Lösung für das Pay-As-You-Drive könnte etwa derart aussehen, dass eine On-Board-Unit zwar lokal („im Fahrzeug“) alle relevanten Daten aufzeichnet, jedoch an das Versicherungsunternehmen nur abstrakte, aggregierte und konsolidierte Daten weitermeldet, die ebenfalls eine individuelle, risikoabhängige Tarifierung ermögli-

chen, mit denen aber weder das Unternehmen, noch Behörden noch Dritte etwas anfangen können. Eine weitere Möglichkeit wäre es, das Pay-As-You-Drive konsequent als Offline-Lösung zu konzipieren: Eine Black-Box im Fahrzeug zeichnet zwar aggregierte Daten hinsichtlich des Fahrverhaltens auf, diese Daten werden aber erst im Falle eines Unfalls vom Versicherungsunternehmen vor Ort am Fahrzeug eingesehen, um die zukünftige Risikoprämie entsprechend anzupassen. Die genannten Systemlösungen würden damit nicht den gläsernen, aber den gehorsamen Autofahrer produzieren, für den die permanente Überwachung seines Fahrstils alltäglich geworden ist.

Dennoch wirft die Verwendung aggregierte Daten aber auch neue Fragen und Probleme auf, zum einen hinsichtlich der Transparenz für den Kunden über Einstufung und Tarifierung in eine bestimmte Risikogruppe, zum anderen hinsichtlich der Möglichkeit des Nachweises von Fehlfunktionen, sind doch auch Systeme der Ambient Intelligence – wie technische Systeme generell – nicht vor Defekten und Fehlern gefeit. Wie reagiert also ein Versicherungsunternehmen, wenn berechtigte Zweifel an der Richtigkeit einer Einstufung vorliegen? Besteht es auf die Korrektheit der Daten oder zeigt es sich einsichtig und kulant? Auch eine Art von Informationsasymmetrie – diesmal zu Lasten des Versicherungsnehmers –; eine Informationsasymmetrie aus Verbraucherperspektive, die in der Fachliteratur so bisher kaum diskutiert wurde.

Zusammenfassung und Ausblick

Die von Entwicklern geäußerte Nutzungsvisionen der Ambient Intelligence im Rahmen betrieblicher Informationsverarbeitung enthalten – wie Nutzungsszenarien generell – unweigerlich explizite und implizite Annahmen über Nutzer und Nutzungsformen, Annahmen, die die spätere Verwendung der technischen Systeme stark vorstrukturieren, einschränken und prägen. Damit ein technisches System später aber auch erfolgreich ist und „funktionierte“, muss es an die alltäglichen Deutungs- und Handlungsmuster der Nutzer und ihrer Umfelder anschlussfähig sein. Aufgabe der Technik- und Medienphilosophie bzw. der Informationsethik ist es daher zunächst, in enger Zusammenarbeit mit unterschiedlichen Nachbardisziplinen die in den Szenarien gemachten Präsuppositionen und das damit verbundene ideologieinduzierte Bewertungsgeschehen zu analysieren, herauszuarbeiten und zu problematisieren. Die Funktionalisierung des Men-

schen als Aufgabenträger und optimierungsbedürftige Humanressource ist hier als Beispiel ebenso zu nennen, wie die umfassende Erörterung der Möglichkeiten und Grenzen risikoadjustierter Versicherungspolizen auf Basis von Ambient-Intelligence-Lösungen und dem damit verbundenen neuen Paternalismus. In einem nächsten Schritt ist es dann Aufgabe der Technikphilosophie und Informationsethik, Vorschläge für akzeptable, gerechtfertigte bzw. rechtfertigbare Problemlösungen zu unterbreiten. Der Verlust an Privatheit wurde im vorliegenden Fall als neuralgischer Punkt sowohl im intraorganisationalen wie auch extraorganisationalen Bereich identifiziert, dem z.B. durch die Verwendung von Selbstlokalisierungstechniken statt Trackingtechniken begegnet werden kann oder aber indem die Systeme konsequent als Offline-Lösungen konzipiert werden bzw. nur auf Basis aggregierter Daten arbeiten. Die normative Akzeptabilität technischer Lösungsvorschläge gibt dann die Basis ab für die spätere, faktische Akzeptanz: Es kann davon ausgegangen werden, dass aus technik- und informationsethischer Perspektive gerechtfertigte Lösungsvorschläge von den späteren Nutzern auch schneller akzeptiert und adoptiert werden. Dies muss jedoch nicht der Fall sein. Es gibt eine Vielzahl unterschiedlicher Faktoren, die die Diffusion neuer Techniken begünstigen, aber auch erschweren oder verhindern können. Die Zukunft wird zeigen, ob die hohen Erwartungen, die in die Ambient Intelligence gesetzt werden, auch erfüllt werden oder ob sich nicht völlig neue, unerwartete Verwendungsweisen dieser Technik durchsetzen. Hierbei ist und bleibt es Aufgabe der Informationsethik, derartige Entwicklungen zu begleiten und kritisch zu reflektieren, um ihrer notwendigen aufklärerischen Funktion im Rahmen gesellschaftlicher Technisierungsprozesse auch nachkommen zu können.

Literatur

- Filipova, Lilia / Welzel, Peter (2005): *Reducing Asymmetric Information in Insurance Markets: Cars with Black Boxes*. Beitrag Nr. 270, *Volkswirtschaftliche Diskussionsreihe, Universität Augsburg*, 2005; verfügbar unter: <http://www.wiwi.uni-augsburg.de/vwl/institut/paper/270.htm>
- Filipova, Lilia (2007): *Monitoring and Privacy in Automobile Insurance Markets with Moral Hazard*. Beitrag Nr. 293, *Volkswirtschaftliche Diskussionsreihe, Universität Augsburg*, 2007; ver-

- füßbar unter: <http://www.wiwi.uni-augsburg.de/vwl/institut/paper/293.htm>
- Fleisch, Elgar / Mattern, Friedrich (Hrsg. 2005): *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*. Berlin, Heidelberg, New York 2005.
- Heesen, Jessica / Siemoneit, Oliver (2007): *Opportunities for Privacy and Trust in the Development of Ubiquitous Computing*. In: *International Review of Information Ethics* Vol. 8 – December 2007, S. 47-52; verfügbar unter: http://www.i-r-i-e.net/inhalt/008/008_8.pdf.
- Horsch, Andreas (2005): *Agency und Versicherungsintermediation*. In: Horsch, Andreas / Meinhövel, Harald / Paul, Stephan (Hrsg.): *Institutionenökonomie und Betriebswirtschaftslehre*, München 2005, S. 81-99.
- Jendoubi, Lamine (2007): *Management mobiler Betriebsmittel unter Einsatz ubiquitärer Computersysteme in der Produktion*, Dissertation, Universität Stuttgart; verfügbar unter: <http://elib.uni-stuttgart.de/opus/volltexte/2007/3195/>
- Lessmann, Peter (2008): *Bespitzelungs-Affäre bringt Telekom-Chef Obermann in Not*. In: *Heise-Online-Newsticker*, 19.11.2008; verfügbar unter: <http://www.heise.de/newsticker/Bespitzelungs-Affaere-bringt-Telekom-Chef-Obermann-in-Not-/meldung/119153>
- Mattern, Friedemann (Hrsg. 2003): *Total vernetzt. Szenarien einer informatisierten Welt*. Berlin, Heidelberg, New York 2003.
- Müller, Christian / Zimmermann, Hans-Dieter (2003): *Beyond Mobile: Research Topics for upcoming Technologies in the Insurance Industry*. In: *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS) 2003*, Big Island/Hawaii.
- Murphy, Martin (2008): *Die Datensammler der Telekom*. In: *Spiegel Online*, 28.9.2008; verfügbar unter: <http://www.spiegel.de/netzwelt/tech/0,1518,580731,00.html>
- Nieder, Peter (1997): *Erfolg durch Vertrauen*. Wiesbaden 1997.
- Oberholzer, Matthias (2003): *Strategische Implikationen des Ubiquitous Computing für das Nichtleben-Geschäft im Privatkundensegment der Assekuranz*. Karlsruhe 2003.
- Persson, Anders J. / Hansson, Sven Ove (2003): *Privacy at Work – Ethical Criteria*. In: *Journal of Business Ethics* 42 – 2003, S. 59-70.
- Phillips, David / Wieglering, Klaus (Hrsg. 2007): *Ethical Challenges of Ubiquitous Computing*. *International Review of Information Ethics*, Vol. 8 – December 2007; verfügbar unter: <http://www.i-r-i-e.net/issue8.htm>
- Rössler, Beate (2001): *Der Wert des Privaten*. Frankfurt a. M. 2001.
- Schwer, Martin / Thies, Barbara (2002): *Vertrauen als Organisationsprinzip*. Bern, Göttingen, Toronto, Seattle 2002.
- Siemoneit, Oliver / Jendoubi, Lamine / Bauer, Martin (2004): *Smart Factory – Mobile Computing in Production Environments*. In: *Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES) 2004*, Boston.
- Siemoneit, Oliver / Heesen, Jessica / Hubig, Christoph / Wieglering, Klaus (2005): *Leben in einer vernetzten und informatisierten Welt. Context Awareness im Schnittfeld von Mobile und Ubiquitous Computing*. SFB 627 Bericht Nr. 2005/05, Universität Stuttgart; verfügbar unter: http://www.informatik.uni-stuttgart.de/cgi-bin/NCSTRL/NCSTRL_view.pl?projekt=SFB-627&id=SFB627-2005-05&mod=0&engl=&inst=
- Siemoneit, Oliver / Lucke, Dominik / Westkämper, Engelbert / Eissele, Mike / Ertl, Thomas (2008): *Privacy-Preserving Self-Localization Techniques in Next Generation Manufacturing. An Interdisciplinary View on the Vision and Implementation of Smart Factories*. In: *Proceedings of the IEEE International Conference on Control, Automation, Robotics and Vision (ICARCV) 2008*, Hanoi.

Paul Wright:

Should corporate management include a Computer Forensics and Incident Response capability into realigned Information Security Principles?

Abstract:

IT enabled abuse and data compromise is a major problem to senior management and organisations as a whole. It has no boundaries, and globally undermines electronic commerce whilst being facilitated by the rapid development of the Internet, computer and information technology. The prevention, reporting, detection and our ability to investigate is of overriding importance to a range of institutions and establishments. Currently the full extent of the problem is not known and at present cannot be scoped; however there is substantial evidence that shows it to be on the increase. Despite historical reports such as the Council of Europe report on Cyber crime (2001)¹⁷ that indicated there would be an increase in criminal offences that exploit the opportunities presented by the globalisation of computer networks.

Agenda

Introduction.....	16
What do we know?.....	17
Trends.....	18
Investigative Ability.....	18
Lack of Intelligence Analysis	19
Incident Response	20
Measuring the Effectiveness of Controls.....	21
Conclusion.....	21

Author(s):

Paul Wright, MSc, EnCE, CFIA, CSTA:

- Organization and contact address: e-crime consultancy, PO Box 4400, Toddington, Dunstable, England LU5 6WE
- Telephone, email and personal homepage: ☎ +44 7973 672918, ✉ paulwright@e-crimeconsultancy.co.uk, 🌐 www.e-crimeconsultancy.co.uk

¹⁷ Council of Europe (2001) CETS No.185 Convention on Cybercrime. Budapest. 23/11/2001Petherick, W. (2001). Criminal Profiling. USA. Crime Library

Introduction

Firstly, it will be argued that senior management should realign the primary objectives of information security from a focus on the principles of confidentiality, integrity, and availability (CIA) to risk and exposure assessments, and vulnerability testing. Secondly, and more importantly, the incorporation of a computer forensic capability, an incident response procedure and the use of digital intelligence within any information security strategy will be advocated. Then, having produced the evidence to support this, a number of recommendations on how to implement such strategies will be proposed.

Information is a valuable asset to any organisation, and those that use it for e-commerce are now being affected by the challenges of IT enabled abuse, in particular data compromise. In some instances the technological developments and innovative mind of the abuser are leaving information security and legal systems playing catch up.

This results in the persistent occurrence of IT abuse and data compromise globally, causing serious financial loss and reputational damage to organisations and the individual. The source of this data comes from large-scale compromise incidents at a corporate level, yet still the spotlight tends to focus upon the individual.¹⁸

The other drawback when scoping IT abuse and data compromise is the fact that the availability of information is limited and all too regularly it is defined anecdotally from a small number of well-known incidents. At other times, questionable, optimistic or negative estimates are presented as fact. Some organisations believe that a thorough and methodical approach to the collation and analysis of compromise incident information will give up a more accurate evaluation of the circumstances and in time will produce a more reliable understanding of this problem.

To protect themselves, organisations need to be encouraged to invest in an Information Security Management System (ISMS). By implementing said systems organisations will at the same time go towards compliance with Principles 2 and 3 of the

Financial Services Authority's (FSA) report in 2007 entitled "*Principles-Based Regulation*".¹⁹ Noting that the FSA clarifies this by stating that all organisations' handling of data in both the public and private sectors can benefit from its advice.

Principle 2 requires "that a firm must conduct its business with due skill, care and diligence."

Principle 3 that "a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

Currently, the main objectives of information management are confidentiality, integrity and availability, not forgetting accountability and accessibility. Do these objectives enable organisations to protect themselves while being able to respond to incidents and disseminate digital intelligence so others can act upon it?

The FSA in their recent report on "*Data Security and the Financial Services*"²⁰ have consolidated examples of poor practice in data security, for example:

1. No training to communicate policies and procedures.
2. Temporary staff receiving less-rigorous vetting than permanently employed colleagues carrying out similar roles.
3. Failing to consider continually whether employees in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.
4. Failing to monitor super users or other employees with access to large amounts of customer data.
5. Firms stockpiling obsolete computers and other portable media for too long and in insecure environments.

Surely a robust e-crime prevention approach and the establishment of e-crime prevention positions could target these areas and more?

¹⁸

http://news.bbc.co.uk/1/hi/uk_politics/7667507.stm

¹⁹ <http://www.fsa.gov.uk/pubs/other/principles.pdf>

²⁰ Data Security in Financial Services 2008 [Online] http://www.fsa.gov.uk/pubs/other/data_security.pdf

What do we know?

Historical evidence on how organised offenders work can be found on the Internet, one incident in particular was when a person using the nickname 'Reverse' was interviewed and he/she stated;

"We have a group of professional hackers/fraudsters/legal bankers, we share information, but if we work together also revenues".

"My name is 'Script', I'm a founder of forum.carderplanet.net and I can provide you with excellent credit cards with cvv2 code and without it, minimum deal is a USD \$200.00" (Script, 2003)²¹.

A report from the Information Assurance Advisory Council (IAAC) claims that companies are not able to collect digital evidence properly, and as a consequence any prosecution is not straightforward. The IAAC have responded by releasing guidelines to assist companies in capturing and preserving electronic evidence in a way that makes it admissible in court. "Effective detection and prosecution have a central role to play in deterrence", said Pauline Neville Jones, Chair of the IAAC (Sommer, 2005)²².

An important point is that organisations and individuals must recognise that whatever analysis they carry out and whatever policies and procedures are implemented, they will quickly become out of date. Moreover, this also includes how the investigator carries out digital analysis of computer media.

In the meantime, very few managers are happy to admit that they have had serious information security issues in their organisations and as a consequence that they must expect there will be more breaches in the future, and they will be harder to detect. As with legislation, the adoption of security controls is not keeping pace with the growing use of new technologies. Organisations are becoming dependent upon a complex web of worldwide infor-

mation infrastructures, without necessarily understanding or quantifying the risks or their exposure to the same.

It is readily acknowledged that some organisations have tried and tested policies, procedures and best practices to combat data compromise. Unfortunately investigative experience shows us that this is not always the case and that there are internal organisational voids and single points of failure that facilitate such compromise.

When an incident occurs there is a strong tendency to have staff 'take a quick look' at the computers involved in an attempt to confirm or deny suspicions. Unfortunately, this act, if not carried out using proper protocols will result in changes to data that damage forensic evidence²³. IT professionals are well informed about their organisations' systems, data locations, media types, software use and data retention policies. Nonetheless, this wealth of information does not give rise to an expertise in the area of e-data compromise or computer forensics.

Illegal on-line techniques and illegal electronic searching of an organisation's data are being used to obtain sensitive documents. The wealth of the supply can be substantiated by looking at the chronology of data breaches available on the privacy-rights.org website²⁴. It indicates the extent of the problem, for example, from January 2005 till January 2009, the said website records a total of over 252,000,000 identities as having been lost. These incidents are mainly located in the United States; on the other hand, if breaches from the rest of the world were included the total number would be appreciably higher.

Recent high profile financial investigations involving global organisations demonstrate the pivotal role that electronic data can play in legal disputes and investigations. Organisations that choose to ignore this vital evidence risk severe reputational damage and financial penalties. These events and the recent

²¹ Script. (2003, January 22) you can buy credit cards on www.carderplanet.net. Message posted FORUM.CARDERPLANET.NET. Retrieved October 18 2006 from <http://lists.debian.org/debian-hurd/2003/01/msg00075.html>

²² Sommer, Peter. (2005) Directors and Corporate Advisors Guide to Digital Investigations and Evidence. Information Assurance Advisory Council www.iaac.org.uk

²³ ACPO (Version 4.0) Good Practice Guide for Computer based Electronic Evidence, Association of Police Chief Officers. [Online] http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

²⁴ <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>

loss of data from the Child Benefit Agency²⁵ and the Nationwide Building Society²⁶ have raised the growing profile of identity theft and what it can cost a company. The FSA fined the Nationwide £980,000.

The focus to date has been on how individuals can protect themselves by shredding documentation and showing extra caution when divulging personal details. However, while rising levels of consumer awareness should be welcomed and encouraged, the focus on the individual is not the way forward. One of the major sources of customer information for the offender comes from large-scale data compromise and identity theft incidents at a corporate level.²⁷ Confidential data such as consumer details, intellectual property and financially sensitive information all have a fundamental value.²⁸

It is important to note that when missing data is retrieved, if the data was not protected i.e. encrypted, there is no assurance that it has not already been duplicated, stored elsewhere, or forwarded to another for illicit purposes. In addition, in 2007 data loss was reported to be the most common type of financial crime reported to the FSA, who also judged it to be highly likely that many data losses are not identified or go unreported.²⁹

Trends

Firstly, a large number of organisations are failing to recognise all aspects of the security risks that they are exposed to. Some just do not realise the magnitude of the risk, while others do not have the know-how to mitigate their vulnerability and countless fail to provide sufficient resources to lessen the risk.

Secondly, the enormous volume of data concerned in a typical compromise incident practically assures

that those involved have a plentiful supply of information and intelligence, which is the foundation for many illegal endeavours. This endless supply of high quality data virtually guarantees that for the foreseeable future IT abuse and data compromises will remain a profitable business. It is also useful to recognise that immoral individuals will respond to opportunities rapidly and tend to exploit emerging opportunities much faster than most organisations can design and implement security controls.

Then there is a 'reputational damage' bias in any statistics. This is due to the fact that a significant number of organisations consistently fail to report information and therefore cause an under representation in the available figures. Additionally, those developing organisations that lack any Information Security Management System (ISMS) have an inadequate ability to detect and report data compromises.

More recently, we have seen another trend where security cleared staff contravened internal policies and procedures by looking at information relating to celebrities, committed fraud or were coerced into giving data to criminals or allowing them access to the same.³⁰

Investigative Ability

IT abuse and data compromise is committed across cyberspace and does not stop at national borders. More than with any other global crime, the swiftness and flexibility of IT abuse and data compromise challenge the existing rules of regulation and legislation. It can be perpetrated from anywhere in the world against any computer, and it is recognised that efficient action to combat it is necessary at not only a local level but also at a global level.

Legislation has fallen behind; it needs to maintain the same speed of change as *"Moore's Law"*³¹. The international legal systems have gone some way to achieve this with the sixth principle³² established by G8, commonly known as *"Quick freeze, slow*

²⁵

http://news.bbc.co.uk/2/hi/uk_news/politics/7104840.stm

²⁶ <http://news.bbc.co.uk/1/hi/business/6360715.stm>

²⁷ <http://news.bbc.co.uk/1/hi/uk/7449927.stm>

²⁸ <http://money.aol.co.uk/credit-report-centre/bank-details-sold-on-internet/article/20071203012409990001>

²⁹ Page 15, Data Security in Financial Services 2008 [Online]
http://www.fsa.gov.uk/pubs/other/data_security.pdf

³⁰

<http://www.guardian.co.uk/world/2008/mar/21/barrackobama.uselections2008>

³¹ http://en.wikipedia.org/wiki/Moore%27s_law

³² Meeting of the Justice and Interior Ministers of the Eight December 9th -10th, 1997

*thaw*³³. Despite this the detection and punishment of cybercrime is highly likely to remain problematic.

Then consider that alongside the fact that, despite a clear need for consistent legislation around the world to facilitate international investigations, there are major differences between the legal systems and cultures, making legislative consistency difficult. The implementation of '*Corpus Juris*' is a long way off.³⁴

Organisations are becoming dependent upon a complex web of global information infrastructures, without necessarily understanding or quantifying the risks. The damaging results of an incident can be minimised if an organisation is pro-active and innovative in putting itself in a position to lessen the cost of any investigation, and penalties that are related to the exposure of valuable data. The scope of the problem may be larger than first perceived and untrained staff may overlook significant lines of investigation, which then leaves the organisation vulnerable to a reoccurrence of the same incident. Therefore, policies need to be established with regard to company computers and networks to provide a line of authority for the conducting of such an investigation.

As always, the quandary of target-based investigations is that funding decisions are based on tick box results, good clear-up figures and value for money. By contrast, there's little or no motivation to invest in e-crime investigations and forensics when the offences are extremely complex to investigate and the probability of a successful conclusion are restricted, especially as offenders and evidence are often located overseas.

³³ "Quick freeze, slow thaw" arrangement by which law enforcement and judicial bodies can fulfil their procedural obligations under domestic law for release of information to foreign law enforcement or judicial officials without risking the loss of critical data.

http://media.hoover.org/documents/0817999825_35.pdf

³⁴ Wikipedia. Corpus Juris. The legal term Corpus Juris means "body of law". It was originally used by the Romans for several of their collections of all the laws in a certain field. Retrieved October 18 2006 from http://en.wikipedia.org/wiki/Corpus_juris

Peter Sommer has responded to Minister Hazel Blears recent announcement of £70 million spent on funding websites to target Muslims in a bid to counter the threat of web-based extremism³⁵ by stating, *"How can that sort of money be justified when there are areas of e-crime crying out for cash, but not getting a penny? It's outrageous,"*

Previous investigations and business presentations can confirm that organisations could do more and are definitely vulnerable to e-crime and IT abuse. Would an e-crime advice centre linked to the chamber of commerce be a way forward? Has the National e-Crime Prevention Centre (NeCPC) got it right?³⁶ Will we be playing 'catch-up' when the Police Central e-Crime Unit (PCeU) is established in 2009?³⁷

Lack of Intelligence Analysis

Many make out that there are limitations to the information and intelligence that can be gathered; there is not, there is only a need to balance, risk assess and evaluate one's ability to gather digital intelligence – know thy enemy.

In these circumstances, knowing your foe is no longer an option – it's a necessity. If organisations do not know their enemy and are unaware of current trends and techniques, it becomes difficult to see how effective controls, procedures and policies can realistically be put in place. For example, how many organisations routinely harvest the criminal intelligence that is openly available to anyone with access to the Internet? How many organisations know how to monitor criminal data markets so that they can see if any of their corporate data is being offered for sale, thus indicating that they have had a security breach? In addition, without an understanding of the way the high-tech abuser thinks, it becomes difficult to anticipate future attacks.

This is where senior management has to have an understanding of the offender's modus operandi for

³⁵ "Political Pain". PC Pro 8th February 2008 <http://www.pcpro.co.uk/features/164145/the-ecrime-epidemic/page3.html>

³⁶ <http://necpc.org.uk/>

³⁷ <http://www.computerweekly.com/Articles/2008/09/30/232508/government-pledges-funding-for-e-crime-unit.htm>

acquiring data. This in turn will lead to a logical conclusion that international coordination and collaboration are not the only ways to address data compromise.

There is hard intelligence that data markets exist and are expanding and it is compounded when you combine this with the fact that the sheer volume of data involved in a typical compromise guarantees that the criminal has an abundant supply of individual and corporate information.

In addition some organisations have implemented a retrospective move towards information and data security risk assessments, and exposure assessments. They need a breach of security or data loss to have taken place before considering such risks, exposure and procedures to deal with the same. Without these, organisations will allocate their assets improperly and expose themselves, their clients and customers to preventable risk.

It is also worth noting that currently the works of those who produce investigative guidelines for e-crime tend to focus on detection and prosecution. They cover the specialist forensic and investigative work that is required to tackle IT abuse and e-crime, but give little attention to the area of e-crime prevention and intelligence analysis.

Incident Response

According to the ISO standard, *"information security is achieved by implementing a suitable set of controls"*³⁸. It goes on to recommend that an organisation should establish procedures *"to ensure a quick, effective and orderly response to security incidents"*. These procedures should guarantee the reporting of an incident to an appropriate authority. The organisation that has suffered a security incident must properly collect evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings.

This requires that the evidence be collected in a forensically sound manner. The standard recognises this explicitly, as it notes that an organisation *"should ensure that their information systems comply with the requirements applicable to the production of admissible evidence. Indeed, to achieve*

*quality and completeness of the evidence, a strong evidence trail is needed"*³⁹.

If an organisation does not have the tools necessary to collect evidence in a manner that preserves its admissibility it risks compromising its legal, and as a consequence its financial situation.

When an incident is detected initially, it may not be apparent that it will result in civil or criminal court proceedings. Therefore, the danger exists that necessary evidence is destroyed accidentally before the seriousness of the incident is realised. Best practice utilises the standard to improve current information security controls and measures. An organisation must decide which strategy is most appropriate to match its business needs.

The integration of network and computer forensics into an information security programme can limit the exposure of critical and sensitive data in the event of a security breach. It can also facilitate an appropriate reaction and warning procedure so as to reduce exposure and liability.

A lack of understanding about computer forensics means that organisations are highly likely to handle any potential evidence in an improper manner. Such evidence needs to have been acquired in a forensically sound manner; failure to comply with the appropriate evidential handling procedure, civil or criminal, can result in no formal action being taken against a perpetrator. Note that criminal proceedings require a higher degree of proof.

The importance of forensic awareness and the employment of computer forensics when responding to an incident cannot be emphasised enough. Those that do prepare will put themselves ahead of the game when it comes to reducing costs and liabilities associated with the exposure of data.

Therefore extra investment in security, incident response and computer forensics is worthwhile, especially as many are now remarking on how the increased use of computers to commit offences produces a significant volume of electronic evidence for both civil and criminal proceedings. This in turn is causing problems to investigators due to the numerous places in which evidence can be located,

³⁸ <http://www.27001-online.com/>

³⁹ ditto

and the ease with which such evidence can become contaminated.⁴⁰

*"If there is even the slightest chance that your may prosecute an individual or organisation based on evidence obtained during your forensic investigation, I highly recommend that your obtain assistance from qualified forensic analysts and/or technology minded law enforcement officers."*⁴¹

Measuring the Effectiveness of Controls

So we need to be able to define how to measure the effectiveness of the selected controls, and to specify how these measurements are to be used to evaluate control efficiency to produce comparable and reproducible results. In other words, measuring the effectiveness of controls to verify that security requirements have, and can be been met.

One such tactic that can be successfully deployed is to conduct a focused exposure assessment to help identify areas where organisations are most exposed to the threat of data compromise. Exposure assessments are designed to get under the skin of potential control weaknesses and to examine existing control regimes with a view to identifying opportunities for unlawful activity. However, if there is not a genuine understanding of the way that criminals operate in this arena, then many potential control weaknesses may go undisclosed.

One way to benchmark data security is to use an International worth standard such as ISO 27001, a security management standard that was introduced in 2005 by the FSA.

Conclusion

Today, there are more organisations experiencing IT abuse and data compromise than ever before, and there are a wider variety of information security systems being breached. To go some way to fighting this, a significant number of organisations need

to take steps to develop their incident response⁴² procedures by improving their policies and forensic capabilities.

A business operating in multiple countries has to comply with a number of different and sometimes-contradictory legal constraints. This is a burden to an organisation and unfortunately it is highly unlikely to change in the anticipated future. Therefore if others are not going to provide legislative protection, we need to be groundbreaking and implement innovative organisational policies and procedures. We believe that realigned information security principles are one way of achieving this cross border, cross-jurisdictional problem, combined with the implementation of incident response.

This issue is a very important one from an organisational perspective because not only are there many legislative drivers regarding information security, there is evidence to show that share price is affected after a security breach and/or a data compromise incident being declared.⁴³

One of the key reasons given by respondents to security surveys for not reporting data compromise and other hi-tech security breaches was the concern for reputational damage.⁴⁴ Therefore why not attack this cross road of ideals from another angle; join together in establishing a coordinated approach to the hi-tech and e-crime aspect of prevention and have all promote the implementation of pro-active policies and procedures in relation to information security management, whilst strengthening them with a forensic and incident response capability.

History validates such a strategy when you consider that many organisations are unaware of how readily the information intruder will exploit weaknesses and

⁴⁰ Clark, Andrew J. (2004). Solicitors Journal. Vol.148 no. 24 Supp (Expert Witness Supplement Summer 2004) pages 14, 16

⁴¹ Chappell, Laura. 'Introduction to Network and Local Forensics.' [Online] <http://www.packet-level.com/pdfs/TUT186-Forensics.pdf>

⁴² Study by Verizon Business Risk Team entitled '2008 Data Breach Investigations Report', recommended the creation of an incident response plan. [Online] <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>

⁴³ February 2005 to June 2006 – Hydrasight and Enterprise Management Association (EMA) examined stock prices of companies who had disclosed an information security breach and found that their shares fell by 5% within a month and did not recover pre-incident for nearly a year.

⁴⁴ <http://www.gocsi.com/press/20050714.jhtml>

how easy it is for them to subsequently, sell, trade or use that data for a range of unlawful activities.

"Clicking on the above links will lead you to the illicit underworld of the Internet" (Internet.com)⁴⁵

Despite all current legislation and regulation, as well as organisational adherence to best practice, policy implementation and recognising standards, there is still:

1. A continued growth in criminal data markets
2. An increase in the reluctance to report IT abuse and data compromises
3. A growing risk to reward\punishment ratio for e-crime
4. A challenge for all organisations to keep up with the advances in technology
5. Contrary to the Information Commissioner's stance, data being taken offsite on laptops and other portable devices⁴⁶
6. A failure by organisations to acknowledge that any security breach that leads to data loss is their responsibility.

However, what is likely to further the private sector's ability to investigate IT enabled abuse is the thought of legal sanctions. This will be an increasing motivator that will cause organisations to consider the establishment of electronic management, the implementation of new security principles and the establishment of an e-crime department, because if we do not take action we will fall ever further behind the offender instead of getting as close as possible.

At the same time it is key to acknowledge the advancement already being made, it remains essential that such progress does not remain predictable and that all concerned look to introduce new and innovative measures, for example:

1. Prepare IT systems as a source of evidence by having a forensic capability and prepare

staff to be able to respond to hi-tech incidents. At the same time support them with achievable, efficient and effective control policies and procedures.

2. Establish E-Crime Departments to fill the gap between IT Security and General Investigation Departments, or ensure that they have a third party e-crime capability.
3. Regular reviews and practice of security controls so that they keep pace with the growing illegal use of new technologies.
4. Introduce policies and procedures for the collection and seizing of electronic evidence, and these in turn should be incorporated into any incident response policy.
5. Bring in pro-active hi-tech crisis management so as to identify those who use technology for an unlawful purpose, in particular IT abuse and data compromise.
6. Understand the offender and keep up with their techniques through the use of digital intelligence.
7. Make sure that data is effectively protected from loss or theft.
8. Have designated individuals identified who will ultimately take responsibility for the final accountability of any breach of security and/or loss of data.

The implementation of such measures will cause to be put in place a new and positive approach to protecting data and an opportunity to set up an early warning system that will inform us when compromised data is being bought, sold and used for illegal purposes.

⁴⁵ Internet.Com, E-commerce. (2002, September 20). The Great Credit Card Bazaar. Retrieved October 18, 2006 from <http://www.internetnews.com/ec-news/article.php/1467331>

⁴⁶ www.ico.gov.uk

Roland Bardy and Arthur Rubens:

A Comparative View of Business Ethics and Governance in the U.S. and Continental Europe

Abstract:

The paper contrasts the economic, ethical, and organizational differences in the U.S. and Europe, as well as the differences in governance and leadership between U.S. and European managers, and how these differences impact decision-making and governance of U.S. and European businesses. In addition, the paper explores and contrasts select ethical and cultural issues between managers on both sides of the Atlantic. It is the authors' view that on both sides of the Atlantic we embrace the call for more ethics in our lives and we expect it from our business leaders and our business dealings. However, in the markets we consistently have seen a short-term orientation of corporate outcomes. It is hoped that there will be a silver lining to the current economic crisis that will help move us away from this position which makes things like ethics, long-term virtues, fairness, all nice to talk about but somewhat estranged from the realities that are practiced in businesses. It remains to be seen if U.S. organizations, business schools and business leaders will change this current position more rapidly than in Europe. The authors are confident, however, that businesses and governments on both sides of the Atlantic will make all efforts for a pronounced transition to integrate ethics into the real strategic thrusts of conducting business.

Agenda

Introduction.....	25
A View on Issues of Business Environment	25
The Legal Environment.....	27
Models of Corporate Governance	28
Managing for Compliance and Integrity	28
The ethical contextualization of business relations.....	29
The relation to customers/consumers	30
The relation to competitors	31
The supplier relation.....	32
The employee's relation.....	32
Government relations	33
Leadership.....	33
Summary and Implications	34

Authors:

Dr. Roland Bardy:

- Organization and contact address: Adjunct Professor of International Management, Fachhochschule Worms, Germany
- Telephone, email and personal homepage: ✉ rbardy@t-online.de
- Relevant publications:

Bardy, R., A. Rubens and J. Schoenfeld: „Business Ethics and Legal Environment of Business in the U.S. and in Continental Europe“. In: Journal of Business Disciplines, 1527-151-X, Vol 1(2); 2008, pp 1-35.

Dr. Arthur Rubens:

- Organization and contact address: Associate Professor of Management, Florida Gulf Coast University, Fort Myers, FL
- ✉ arubens@fgcu.edu

Introduction

Historically there has been a history of pronounced divide of governance and legal systems between the Nordic states and the United Kingdom on the one end and Continental Europe on the other end. The US approach has been nourished mainly from the U.K.; however, contrasting views on how corporations should be managed and overseen have evolved. These differences greatly effect how CEOs look at issues such as governance, accountability, and strategic decision-making, as well as a host of corporate and ethical issues ranging from CEO compensation to how the CEO and the companies deal with competitive intelligence, intellectual property rights, employee privacy, and customer relations.

Recent events such as the meltdown of our financial markets, corporate bailouts, as well as the infamous corporate scandals such as the Enron catastrophe, the corruptions at WorldCom, Tyco, Vivendi, and Royal Ahold, as well as the passage by U.S. Congress of the Corporate and Auditing Accountability, Responsibility, and Transparency Act of 2002⁴⁷ have all served to radically change public and business expectations of corporate accountability. They have brought issues such as business ethics, corporate governance and CEO compensation to the forefront of the business and political agenda^{48 49 50}. Increasingly, the ethics and decision-making practices of CEOs in the U.S. and Europe are coming under greater scrutiny as more and more CEOs are accused of corporate wrongdoings, and as our businesses and organizations on both sides of the Atlantic are faced with stiff competition from a global market and are required to do more for their customers with fewer resources. In addition, this recent turmoil in the world financial markets has only resulted in solidifying public opinion of the need for change in our corporate boardrooms and how CEOs are to govern. The U.S. and European CEOs in the future are faced with a very different business environment than CEOs of only a few years ago. Issues such as volatile economic and social systems, changing expectations of employees and consumers, cost-containment pressures, and the growing do-

minance of China and Asia confront the new managers in the U.S. and Europe and challenge his or her decision-making ability to make equitable and fair decisions, and how to survive in the future. From there, it is hoped that dealing with all these issues will become more ethical. But it is assumed that the differences among Western countries in ethical practices and ideology will remain and will produce different outcomes.

A View on Issues of Business Environment

The focus and the challenges of business ethics in Continental Europe today must be viewed from the perspective that has evolved after the breakdown of communism. Democracy is new in many countries of Europe, and even though the concept of democracy is European as it was invented in the city state of Athens some 2500 years ago, there is a much longer tradition of democratic values in the U.S., and the types of constitutional set-ups which prevailed in Europe and which have helped to form the business environment are very different from what we have in the U.S.

Exhibit 1 shows a list of where business issues differ between the U.S. and Continental Europe. Foremost is public administration. With regard to how far public administration stretches here and there, one statistic "shows it all": According to an Organization for Economic Co-Operation and Development (OECD) source, total cost of government as a percentage of GDP were: In the US 33.5, in the UK 55.9, in Germany 55.7, in Italy 59.3, in France 54.0, in Sweden 66.7; the EU average was 51.0. This overall difference explains why the legal environment of business must be different. Also, where we have *uniformity* in the issue we might still find *differences* in attitude. For example with the issue of human rights, as long as there was *Apartheid* in South Africa, US firms withdrew, European firms remained. While there are still US-sanctions against Cuba, EU politicians favor "humanitarian aid," and while the US generally prefers a "hard diplomacy", Europe deploys a much softer and very different type of diplomacy. Yet there is a common base for both, and one may trace it back to Adam Smith who, long before publishing "Wealth of Nations", delineating the goals attained by the *homo oeconomicus*, wrote "The Theory of Moral Sentiments" where he depicted the *homo moralis*. One may hold that there is a transatlantic divide in determining which is the proper balance of the two attainments,

⁴⁷ Sarbanes-Oxley 2002

⁴⁸ Vershoor 2006

⁴⁹ Hasson 2002

⁵⁰ Roberts 2002

but there will always be an agreement on what extent this balancing is acceptable.

Exhibit 1 Issues that Demonstrate Differences/Uniformity of Business Ethics in US and Europe:

Differences	Uniformity
Focus of Public Administration	Human Rights
System and Curriculums of Education	Free Market
Sensitiveness to Stock Price-Effects	Deregulation
Corporate Governance	Child Labor
Legal System	OECD Code for Multinationals
Labor Law	WTO (GATT) TPS
Consumer Protection	GATS
Privacy Protection	TRIPS
Workplace Protection	Sustainable Development
Job Rotation	Responsible Care
Organizational Transformation (M&A, Spin-Offs)	Bribery
GAAP: Rules-Based; IAS: Principles-Based	Insider Trading
Energy Consumption	Trust within Business Relations

There are three other, more practical, consequences which may be gleaned from the contents of Exhibit 1: First, from the outward evidence for a preference of rules-based approaches in the U.S. (over the principles-based approaches in Continental Europe) as in matters like GAAP and, more generally, Corporate Governance, we may infer that this has a foundation in ethical approaches which are slightly

more instrumental and rules-based in the US⁵¹. Secondly, as trust is a common denominator on both sides of the Atlantic with slight variances within Continental Europe⁵², legal barriers to the global

⁵¹ Gibson 2007, Ferrell et. al., 2006

⁵² According to the prominent American philosopher Yoshihiro Francis Fukuyama (The End of History

knowledge economy are bound to fail and even the Commission of the European Union will eventually ease its prohibitive Privacy Rules⁵³. And thirdly, as legal provisions have a much wider reach in Continental Europe, e.g. in Labor Law, the spectrum of guidance in the US will more often mix ethical and legal compliance.

The Legal Environment

Law is inherent in ethics and in how businesses operate. A basic difference between US/Anglo-Saxon and Continental European practice is that the US and the UK apply case law; while on the continent we have a dominance of code law. Then, there is the judiciary: One topic of almost antagonistic layout is that of the competencies of courts. Courts have ample jurisdiction in the U.S., while in continental Europe there is a variety of special courts apart from the ordinary courts such as the labor courts, social courts, and administrative courts. A related topic is that U.S. standing rules allow greater access. For example, in Europe, a case will only be accepted by a court if there is an 'individualized impact', while a case will "stand" before a US- court if whatever infringement of law can be demonstrated. So, while suits to compel administrative action are a normal procedure in the US, in (Continental) Europe cases of administrative inaction are taken to court less frequently than in the US. The Europeans, generally, give priority to a stable political consensus on regulatory matters by prior consultation. In addition, in Europe there are many patterns of tightly knit state-society-relations and the state organizes social interests into large representative hierarchies. This is often called a "corporatist" environment, and it relates to another issue, i.e. that of employee representation and co-determination: Union laws in the

US are not as compelling as in Europe. Even if this may probably change under the new democratic administration and the democratic congress from 2009, the change will never reach as far as, e.g., labor law in Germany, where co-determination is not only executed on the shop floor level but also in the boards, where trade unions and employees representatives have voting rights. This explains why there will always remain fundamental differences in how corporate governance is organized and practiced.

The legal environment in the former communist states of Central and Eastern Europe (CEE) is still to be developed further. But what matters more is that an underlying ethical foundation like Immanuel Kant's (1724-1804) Categorical Imperative ("*Act only on that maxim by which you can at the same time will that it should become a universal law*") would be implanted in the CEE states. This would also encompass the fundamentals of what Karl Popper (1902 – 1994) called the "*Open Society*" and what F.A. Von Hayek (1899 – 1992) called the "abstract rules" of "*Just Conduct*" (i.e. honoring property rights and contracts). In practice, however, there is not enough emphasis on ethical issues in the process of what the politicians call "homogenizing the rules throughout the EU". For the time being, however, more emphasis is placed on reforming the business laws, on introducing all facets of capital-market-constitution and non-intervention. It seems that the task of dispersing knowledge on "western" business procedures and (ethical) responsibilities is much more taken up by U.S. businesses and U.S. business schools⁵⁴. From that side of the Atlantic also comes the ethical concern of John Rawls (A Theory of Justice - The Ethics of Distribution; 1973): Welfare of mankind still requires control through a set of (fair) rules. Welfare can only be distributed justly if a society, by such fair rules, minimizes the effects of its member's accidental circumstances (intelligence, physical strength, social status). Rawls' ideas may seem to be a representation into the legal of what was expressed philosophically by Jeremy Bentham (1748-1832), the English father of *Utilitarianism* ("...an action is good if it produces ... the greatest amount of satisfaction for the greatest number of stakeholders affected by the action"). But welfare, according to Rawls, is not just benefits, it is about "primary social goods", which includes the notion that justice (fairness) and self-respect are prior to questions of mere satisfaction. This certainly is a fundamental ethical principle to be

and the Last Man 1992), the US, Germany and Japan are 'high-trust' societies, while Italy, France, Korea, Taiwan are 'low-trust' societies. He has tested his thesis, and while his findings are that spontaneous sociability – one element of trust – makes for economic growth as it establishes orderly industrial structure, he attributes a higher grade to cognitive trust. Cognitive trust is inherent in network organizations and this will give a natural advantage to those societies that have a high degree of trust (Fukuyama 1995). In this, we have what we might call a „partial divide“ throughout Europe.

⁵³ Di Norcia 2002

⁵⁴ Melloan 2005

divulged in the new CEE democracies, because if any pluralistic community reaches consensus on this, it will achieve political accord.

Models of Corporate Governance

The main differences between the US and the continental European models of corporate governance are shown in Exhibit 2:

Exhibit 2 Models of Corporate Governance

Traditional	Co-determination	Stakeholders Model
Stockholders	Capital and Labor	Social/political/economic interests
Board of Directors	Supervisory Board	Stakeholders in Board
Managers	Management Board	Managers
Employees	Mgrs/Employees	Employees

While the traditional US model of corporate governance features a "one-tier" structure (there is one layer of supervision between stockholders and managers, and this is the board of directors), the continental model of co-determination has two tiers; a supervisory board and a management board, with capital (shareholders), and labor (unions and employees being represented equally in the supervisory board). Some economies in Eastern Europe have set up what is commonly referred to as a "*Stakeholder Model*" which is also practiced in Northern Europe. It includes social, political and economic interests in the oversight and in the board levels.

There are advantages and disadvantages in both structural layouts of corporate governance. But on both sides of the Atlantic, the ethical dimension remains the same: Accountability is foremost, and "Corporate Citizenship", as well as "Corporate Social Responsibility", though first coined by US corporations, have soon become a commitment in Europe. Going even further, some European countries, e.g. Italy and Austria, have copied the US model of sanctioning corporate crime⁵⁵ by establishing ambitious legal frameworks for corporate criminal re-

sponsibility⁵⁶. Also, the systems and procedures for internal control, compliance and risk management have become universal with global application of the COSO model (COSO = Committee of Sponsoring Organizations of the Treadway Commission on Corporate Governance) and of GRC Software (GRC = Governance, Risk Management and Compliance). It is self-evident that risk management entails an ethical dimension, because if a business avoids unacceptable and worrying risks it also acts responsibly towards all stakeholders.

Managing for Compliance and Integrity

Being accountable and being responsible implies that officers on all levels of the corporation are not only able to account but also required to render accounts. In this sense, accountability is part of the normative social order of any community or institution. Corporate governance must provide an appropriate framework of reporting routines, systematic assessment and approval procedures etc., and the moral significance of accounting practice must be upheld and regained, not least because of the prominent role that accounting representations have played in recent corporate scandals. Beyond man-

⁵⁵ The US Federal Sanctioning Guidelines of 1991, apart from setting rules for federal judges, have also spurred the divulgence of corporate guidelines and standards on compliance, both legal and ethical

⁵⁶ Hefendehl 2001

agement accounting, financial accounting and financial auditing (where substantial reforms are under way with the Sarbanes-Oxley Act and with the 8th European Directive that governs the audit profession), reporting and auditing on ethical and social issues is becoming mandatory in the global environment. One background is the negative attention attracted through consumers, media and non-governmental organizations on, e.g. apparel distributors such as Nike, Levi Strauss, Benetton, Adidas or C&A⁵⁷ for questionable procurement and production practices. Another background is the efforts of innumerable institutions establishing internationally accepted standards such as SA 8000, AA 1000 and the Global Reporting Initiative (GRI):

- SA 8000⁵⁸ was founded in 1997 and is now under the control of Social Accountability International (SAI)⁵⁹. It is a global, verifiable standard for managing, auditing and certifying compliance with workplace issues, and companies may seek certification through an accredited authorization auditor.
- AA 1000⁶⁰ was created by the Institute for Social and Ethical AccountAbility⁶¹ and its main goal is a so-called "stakeholder engagement". The engagement of stakeholders enables AA 1000 to build confidence and give legitimacy for a good reputation by projecting a defined stance on social and ethical issues.
- GRI is a multi-stakeholder governed institution providing global standards in sustainability reporting and special alignment with the UN Global Compact Principles on Human Rights, Community Impact, Climate Change etc.⁶².

The three sets of standards are very different in their respective inherent logic, and adherence to either SA 8000 or AA 1000 largely depends on the willingness to participate in the audit and certification processes. Information on SA 8000 and AA 1000 compliance is not available publicly. However,

GRI is linked to the Corporate Register Database⁶³, which can be freely accessed and which as today provides 18880 Corporate Social Responsibility reports across 4779 companies.

The evolution of the standards, especially SA 8000, may serve to demonstrate that norms will only be generally accepted if all affected stakeholders were involved in their elaboration through the SAI initiative. There is a close link in this to Discourse Ethics which stipulates that "a norm is valid when its foreseeable consequences ... could be jointly accepted by all concerned without coercion", and that "only those norms can claim validity that could meet with the acceptance of all concerned in practical discourse"⁶⁴. Even though it may be argued that not each and every of all potential stakeholders were involved in the making of SA 8000, SAI's intention clearly is to include all argumentation. The ongoing process of SA 8000 amendments will also improve the formal design of dialogues (SA 8000 explicitly asks for stakeholder discourses). And it could further shift the idea of the goal of communication from the result, as in traditional discourse theory (a German feature), to the process itself (an American feature), promoting the concept of an ongoing moral conversation. This difference (another "transatlantic divide") is not just limited to the procedures of the discourse; the US-based philosopher Seyla Benhabib also criticizes that, traditionally, contemporary moral and political theory makes a sharp distinction between matters of justice and matters of the good life, and that it only places the former in the realm of ethics. Her expansion of the traditional idea has led to the inclusion of questions and experiences belonging to the private sphere into the moral and political domain – a development that will definitely promote the range of social accounting⁶⁵.

The ethical contextualization of business relations

The focus on Corporate Governance is primordial, because oversee, governance and culture influence decision making on all levels. Towards the outside of the corporation, ethical or non-ethical behavior becomes manifest in the contexts of business relations: How does the corporation, how do their

⁵⁷ Preuss 2001

⁵⁸ SAI (Social Accountability International) 2002

⁵⁹ www.accountability.org.uk

⁶⁰ AccountAbility 1000

⁶¹ Ibid.

⁶² www.globalreporting.org

⁶³ www.corporateregister.com

⁶⁴ Habermas 1999

⁶⁵ Benhabib 2004

officers treat its constituencies (or "stakeholders") customers, consumers, suppliers and service partners, its contractors and employees? And are there differences in this between the US and Europe? Does it matter that the central emphasis on ethics subjects tends to be individual actors in the US, whereas in Europe there is a more "pluralistic" view and hence more interest in institutions?⁶⁶ The main issues will be contextualized as follows:

The relation to customers/consumers

All links and activities between buyers and vendors are configured through responsibilities that are based on generally accepted values: Autonomy, Freedom, Justice, Trust, Truth and Well-Being are constitutive of a marketing ethics⁶⁷. They are not unique to marketing, because they also relate to other areas of life. But when used in marketing, they are part and parcel of decisions regarding product development, advertising, market research etc. Advertising and its use of "sex and fear" and of deceptive practices is, of course, a favorite target of moral criticism on both sides of the Atlantic. But the practices differ: In the US, comparative advertising is legal, which it is not in the European Union, whilst the tactic of "bait and switch" (making people believe that a certain product is available and then offer them another, more expensive alternative) is illegal in the US, but it is not prohibited by law in Europe. Deceptive pricing by "no frills airlines" has been criticized by advertising watchdogs all along, but an EU regulation came up only recently. This is also due to data problems and the lack of European-wide information systems in this area. Non-governmental initiatives use much more information economics here. An US example is "Consumer Fraud Reporting", an online service that warns consumers about specific types of financial scams via the internet⁶⁸.

In the US as well as in Europe, the legal framework on pricing and market exchange was largely predicated on the notion of "caveat emptor", or buyer beware, even though the historic foundation of "fair dealing" in the US stems from the "Federal Trade Commission Act" which was created in 1914. From there, protection of consumer rights which erodes the notion of "buyer beware" developed much faster

in the US (e.g. with the 1975 Consumer Goods Pricing Act) than in Europe. EU regulations as well as national legal frameworks which enshrine the right to safe and efficacious products and to truthful measurements and labeling are worded in very general terms and national laws in Europe differ substantially from each other. So, business ethics very often must begin where the law ends. But there will always be gray areas; if we take the example of "healthy food" and "effectual cosmetics", we are very clearly into consumer vulnerability, and this is where the principles of Trust, Truth and Well-Being should govern. As of 2004, the American Marketing Association (AMA) has adopted a "Statement of Ethical Norms and Values for Marketers" which states those and other principles⁶⁹. Similarly, the European Marketing Confederation (EMC) has issued a Code of Conduct⁷⁰. They might work, because both of them expulse individuals who are found not to have abided by the code – a type of sanction which may be deemed to be severe. Again, in the US, severe punishment is much more drastic than in Europe when consumer fraud is taken to court: Applying the 1991 US Federal Sentencing Guidelines, Acme Corporation was sentenced by US court to pay a fine of four times the loss suffered by its customers who were systematically overcharged for damages occurred during the rent of automobiles⁷¹.

A field where a Code of Conduct is successfully employed is market research. The Code of the Market Research Society (MRS), with members in more than 70 countries, is intended to reassure the general public and other interested parties that research is carried out in a professional and ethical manner⁷². But here, again, we might find a transatlantic divide: When it comes to covert research, especially in engaged public observation where a researcher talks to people without revealing who she or he is, the US attitude towards privacy protection makes it more likely for this method to be applied. The method is deemed to be justifiable if it does not produce „unnecessary harm to subjects"⁷³. A case that has made history is that of Toyota in its early US campaigns, when the company used its

⁶⁶ Crane, Matter 2004

⁶⁷ Brenkert 2008

⁶⁸ www.consumerfraudreporting.org

⁶⁹ AMA 2004

⁷⁰ EMC (European Marketing Confederation) 2005

⁷¹ HBR 2003

⁷² MRS (Market Research Society) Code of Conduct

⁷³ Denzin and Erikson 1982

employees to make friends with potential buyers to learn about their attitudes and preferences.

Market research has received new inputs through web-based data collection: Some argue that the explosion in communications technologies has created an *ethical minefield* for individuals and companies⁷⁴. Surely the technology allows the individual to become "invisible" on the Web, or to misuse e-mail and Web-surfing or to illegally copy software, and there is the big question what corporations should do about these abuses all over the world (the answer would be a "matter of degree"). But when it comes to abuses produced by businesses, there is a clear divide on what is "material": The EU Directive on Data Protection limits the secondary use of personal information collected from consumers to a very great extent. By contrast, the US is leaning towards industry self-regulation. Europe may pay a heavy fine for its obsession with privacy. Already severely behind in technology, further restrictions on the growth of the Internet may see technological companies bypass European venues.

The relation to competitors

There is a wide continuum between conflict and collaboration in competitive behavior. Marketing can be seen "as a game, as a war or a social practice"⁷⁵, and ethical issues in dealing with competitors can either relate to aggressiveness or to elimination of the competitive market. Overly aggressive competition will lead to questionable tactics in intelligence gathering, from the clearly illegal patterns of espionage to the more subtle ways of spying. Beyond the competitive intelligence issues, overly aggressive may apply "dirty tricks" that include negative advertising, stealing customers, predatory pricing and even sabotage. In the US, it was only recently that a case has surfaced which involved Coca-Cola employees who tried to sell the Coke formula to Pepsi Cola⁷⁶. But there were much more cases which became known in Europe: Allegations of industrial espionage were versed against Procter & Gamble in 2001. The company had hired private investigators to find out more about Unilever's hair care business⁷⁷. Canal Plus, an encryption service company of the French media conglomerate Vivid, claimed that

NDS, a UK-based technology firm 80 % owned by Rupert Murdoch's News Corporation, had deliberately cracked their security technology, and then it had sent it to hackers in the USA⁷⁸.

Aggressive behavior would also encompass illegal copying of intellectual property rights (IPR). Again, the likelihood of a universal codification of IPR protection is poor (as was shown for privacy protection), because there are different traditions: In Continental Europe, the moral rights of authors are emphasized. The Anglo-American tradition emphasizes economic rights, and the Asian tradition considers copying as a matter of emulation of the master. Still, the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) is a very powerful instrument, but it refers to inter-governmental relations. At least it enables IPR-owners to take action: Microsoft recently reported a major Egyptian IT company to the local Department of Investigation and Protection of Intellectual Property Rights, a task force run by the Ministry of Interior. The company, which has its headquarters in Nasr City, has been working against the law by installing counterfeit Microsoft Windows and Microsoft Office on the computers it sells.

The opposite of aggressive competition is collusion and cartels. And once more, it seems that the long history of Antitrust law in the US (the Sherman Antitrust Act came into force in 1890) prevents US managers from price fixing through multi-firm conduct and concerted action. US courts see multi-firm conduct to have an unambiguously negative effect and judge it more sternly, while the disposition in Europe may be termed to more repugnant to the abuse of a dominant position. E.g., the European Commission is incessantly investigating into Microsoft's bundling of its Media Player software with Windows, while the claim that the big four mobile phone companies were overcharging consumers in the UK has not yet been taken up by the UK Competition Commission. And back in 1999, the world's three biggest vitamin makers, German BASF, Swiss Roche and French Rhône-Poulenc were charged by the US Justice Department for engaging in a massive price-fixing conspiracy long before the European courts took up the matter.

⁷⁴ Mitchell 2003

⁷⁵ Kotler 2000

⁷⁶ www.boingboing.net/2006/07/05

⁷⁷ Financial Times, 31. Aug. 2001

⁷⁸ The Independent, 1. Oct. 2002

The supplier relation

Ethical issues in dealing with suppliers arise on the organizational level (misuse of market power, unfair treatment, unfair advantage) and on the individual level (giving and acceptance of gifts, bribes, hospitality and other inducements). With regard to the organizational, industry seems to move away from the traditional adversarial relationship with its vendors, due in part to the influence of Japanese business where partnership-based approaches prevail. But in retail, unfair treatment happens more often than not: In the highly competitive German foods market, the market leader ALDI earned a very negative reputation when it used its market power in 2007/8 to force milk-producers into accepting a heavy price decrease. Similarly, the British high street retailer Marks & Spencer suddenly dropped one of its long-term UK clothing suppliers, William Baird textiles group, in 1999, thereby ending a thirty-year business relationship. Baird had to close sixteen factories and lay off 4500 workers⁷⁹. Suppliers should legitimately be able to expect loyalty – the specific dealings will have to show what an obligation of loyalty really has to entail.

An issue which pertains to the purchase function but which entails the entire corporation is "Green Procurement", i.e. the selection of products and services that minimize environmental impacts. Other than in Europe, where only a few industries like the chemical and textile businesses perform „sustainable purchase", US buyers, at government institutions and private enterprises, have developed a reputable record in this field across all industries. An example is IBM, which has converted the need to comply with dozens of environmental regulations into a forward strategy. IBM's „Green Strategy" is proactive in limiting the materials it uses in its electronics, and from there it provides environmentally conscious products to its customers, „not from an altruistic standpoint but from a dollars and cents standpoint", because the customers' purchase agents prefer „green products", too⁸⁰.

On the individual level, the topic is not just gifts, gratuities, bribes, kickbacks bungs, sweeteners etc., but also business-supplier negotiation. An ethical approach to negotiation should steer clear of tactics like puffery, weakening the opponent, non-disclosure, distraction and the like. This is not only

because it is the right thing to do but also because such practices can incur costs for the negotiator (costs of rigidity, of lost opportunities, etc.). In all, unethical decision making in this context can very well be limited by limiting opportunities. Opportunities arise from conditions that either provide rewards for or fail to erect barriers against unethical behavior. Opportunity also comes from knowledge: Withholding information or lying to vendors (as well as to customers or employees) is the most common type of misconduct observed in the National Business Ethics Survey (NBES) conducted in the US⁸¹. One remedy lies with information economics: reporting on negotiations, tracing the access to and the use (and misuse) of data will provide solution, as will proper training and socializing newer employees to abide by the rules and norms and the culture of the organization.

The employee's relation

As mentioned before, the participation of employees and their representatives in corporate decision-making is a much wider in Europe than in the US. Apart from the legal background, this is based on the European attitude of decision-making by consensus, and, therefore, employees' rights and duties may be interpreted somewhat differently in the US and in Europe. While the basic rights to freedom from discrimination, to fair wages, to healthy and safe working conditions etc. will be applied similarly, the rights to privacy and to due process (promotion, firing, disciplinary proceedings) are more limited in the US as compared to Europe. This has a downside: Performance monitoring in German corporations often is viewed as "spying on the employees", and one big retailer was recently taken to court on this matter (there was a recent case in German which involved retail giant LIDL). Likewise, co-determination on the board level mixes employee duties (complying with labor contract, respecting the employers' property and values) with the duties, which a board member, who represents a trade union, feels towards this union. In consequence, the other board members might deem it necessary to find out if such an attitude provokes the breach of secrecy. Deutsche Telekom did not see another way out from this dilemma than "spying on employees"⁸².

⁷⁹ The Daily Telegraph, 02. Aug. 2001

⁸⁰ IBM (www.ibm.com): „Big Blue Goes Green"

⁸¹ The Ethics Resource Center 2000

⁸² www.unwiredview.com, 2008/05/26

Spying on employees was also what Boeing meant to be the ultimate resort in November 2007 after a whistleblower was charged with 16 counts of computer trespass for allegedly stealing 320,000 company files and giving some of them to the *Seattle Times* to document flaws in the company's inspection process for one of its new planes. The company estimated that the stolen data could have cost the company between \$5 billion and \$15 billion if the information got into the wrong hands. Boeing set out to restore security to ferret out that type of „whistleblowers“ by videotaping workers and reading their e-mail⁸³. On the other end, when employees raise concerns about work-related issues that are not taken up adequately, they face a plight: Should they „loyally“ accept the situation, or should they blow the whistle? The vast majority of whistleblowing cases are resolved within the chain of command and with the help of human resource management officers⁸⁴. Going to the board or outside the company would only be the last step, but it must be looked at as a part of the system, because „democratic capitalism requires that people trust in the integrity of public and private institutions alike“⁸⁵.

Government relations

Government has a relation with business where both partners are mutually dependent on each other. For government, the main ethical issue here lies in the necessity of carrying out the mandate it has been given by society, and of course one aspect of this is its constraint and enabling of business. And business is entitled to rely on agreements and guarantees issued by governments, and especially by the preceding ones when governments change after an election. All lobbying has its source from that context. While in the US there are more person-to-person contacts (and hence more personal conflicts), the lobbying scenario in Europe is characterized by collective action through business affiliations and associations. Both ways might end up in people occupying a dual role in business and politics at the same time, and if handled professionally, that role could benefit both constituencies. All this is pretty much legal all across Europe and the US,

although some of it may be in the gray area of business ethics. For that, NGOs and other watchdogs should be included in data sharing and reports. If these checks and balances are not in place, business will be lead to buy an influence on regulation, from „state capture“ to outright corruption. Again, there are many means to combat corruption, starting with the UN Convention against Corruption and reaching to national and private institutions like the UK Fraud Advisory Panel, the „Bribe Payers Index“, Transparency International etc., all supported by broad data interchange.

One subject that has many shades of „gray“ is tax evasion. For the sake of conciseness, it will not be covered here.

Leadership

This comparison of how business conditions and values are generated spread and modified within different business environments would not be complete without some considerations on leadership. Can leadership produce values? Or better said, can it just secure that values are observed and adhered to when making decisions?

U.S. leaders are often reproached for being „ethnocentric“ and biased to assume their value system is best⁸⁶. On the other hand, European leaders will often try to avoid uncertainties related with leadership change by „depersonalizing“ management. They will establish a set of „substitute variables“⁸⁷ such as high professional orientation, high coherence within teams, intrinsically satisfying tasks of subordinates, etc., to eliminate „adverse: effects of leadership change. At the same time, the subordinates will set up their own „substitute variables.“ As changes of leaders take place rather often on the international scene when expatriates are assigned and re-assigned to foreign subsidiaries, the international manager must learn how to cope with such „substitute variables“⁸⁸. A topical study has shown⁸⁹ that at least the functional flexibility is higher in U.S. management. Thus, U.S. managers might easier

⁸³ Seattle Post, Nov. 16, 2007

⁸⁴ Treviño and Nelson 2004

⁸⁵ Time Magazine of December 22, 2002, naming the Enron and WorldCom whistleblowers „Persons of the Year.“

⁸⁶ Hofstede 2000

⁸⁷ Yukl 1994

⁸⁸ Harzing 1999, Petersen 1993

⁸⁹ Hewitt-Dundas 1997

find effective solutions to (functional) conflicts in multicultural environments⁹⁰.

Other recent research has ascertained that American leaders are not as individualistic as has often been suggested⁹¹. It has been shown that U.S. businesses are highly characterized by an egalitarian commitment^{92 93} even though they mostly have a command and control orientation with a top-down management approach. While this orientation may promote the view that employees may be used instrumentally towards the objective of the organization's executive to "create wealth," it is the conceptualization of 'egalitarian commitment,' the wide-spread endeavors of cross-cultural training and an increasing U.S. engagement in transition economies which have modified and 'softened' American instrumentalism.

The positive picture of US leadership traits has been radically changed by the Enron catastrophe, coupled with the simultaneous scandals at Worldcom, Tyco, to name a few. This has served to radically change public and business expectations of corporate accountability and the ethics of the corporate leaders^{94, 95, 96}. For many years the CEOs of the U.S. when compared to their European counterparts made dramatically more in compensation and earnings. Throughout the 1990's, U.S. CEOs' executive packages soared, and many executives won guarantees of big rewards whether or not their businesses succeeded. In the early part of this decade, European CEOs started to demand greater salaries and compensation packages. However, recent ethical scandals on both sides of the Atlantic as well as the financial crisis have lead to public outcry against CEO salaries. For example, the chief executive of a Standard & Poor's 500 company made, on average, \$14.2 million in total compensation in 2007, according to preliminary data from The Corporate Library⁹⁷. However, this type of executive compensation has become unacceptable as the public became aware of the large severance packages given to

CEOs of companies at the center of the mortgage crisis.

Summary and Implications

Although there are organizational and philosophical differences in how U.S. and European CEO's regard governance and ethics, it is imperative that business leaders on both sides of the Atlantic adhere to a code of ethics, and be pragmatic in their management practices and decision-making, especially in light of the current challenges in our financial markets. Ethical issues in business require norms that may very well be based on rational arguments, but their specific content must be generated from real-life experiences rather than belief systems. This argumentation of Discourse Ethics, as we have seen from the example of Social Accounting standards turns out to be a powerful principle: It is all about stakeholder engagement, which is the core of all social standards. ("A norm is valid when its foreseeable consequences ... could be jointly accepted by all concerned without coercion", and "Only those norms can claim validity that could meet with the acceptance of all concerned in practical discourse".⁹⁸ Thus, the dilemma of weighing ethics versus effectiveness on an individual level becomes resolved because it is moved up to a communal level where the criteria for decision-making are contributed through interaction. And with this we can very well find a pathway (not far from Adam Smith's, but probably the other way round) from "Homo Oeconomicus" to "Homo Reciprocans" to "Homo Moralis"⁹⁹ For the practitioner, this explains why "Good Ethics" means "Good Governance" and also "Good Cost Control" through minimizing risks, avoiding fines, court-imposed remedies and criminal charges, reducing operational costs by properly handling environmental and workplace issues, avoiding loss of business and enjoying a greater access to capital¹⁰⁰: Business ethics is the challenge of ensuring that the enormous entrepreneurial energies released by today's free-market global economy end up by serving society and not destroying it.

Ethics, as stated by Kent Druyvesteyn, who was vice president for ethics at General Dynamics from 1985 to 1993 and one of the first ethics officers in an

⁹⁰ Ravlin, Thomas and Ilsev 2000

⁹¹ Bond 2002

⁹² Schwartz 1994

⁹³ Smith et al. 1996

⁹⁴ Hasson 2002

⁹⁵ Roberts 2002

⁹⁶ Verschoor 2006

⁹⁷ www.aflcio.org/corporatewatch/paywatch

⁹⁸ Habermas 1999

⁹⁹ Lenz 2008

¹⁰⁰ Mitchell 2003

American company, is „about conduct, from moral awareness to moral judgment to ethical decision making, and not about philosophy“¹⁰¹. But many executives, today, for good reasons, are also embracing the main theoretical foundations as this enlightens awareness and judgment. One proof of this would be the highly positive acceptance and the wide spread of the English version of Peter Ulrich's book "Integrative Economic Ethics"¹⁰² in the US. Ulrich, the leading German-speaking writer on the subject (the book is in its fourth edition in the original German version), progresses through a series of rational and philosophical arguments to address foundational issues and moving business ethics into the realms of political theory and civic rationality. No business leader will be able to neglect Ulrich's argument that corporations exist to serve human demands, and that human' demands are formed by society. So businesses will have to adopt a conduct to serve this principle.

References

- AccountAbility 1000* (<http://www.accountability21.net>): AA1000 AccountAbility Principles Standard 2008
- AMA (American Marketing Association) Statement of Ethics 2004, retrievable from <http://www.marketingpower.com>
- Benhabib, S., *The Rights of Others: Aliens, Residents, and Citizens*. Cambridge University Press, 2004.
- Bond, Michael Harris, et al., "Social Axioms. The Search for Universal Dimensions of General Beliefs About How the World Functions". In: *Journal of Cross-Cultural Psychology*, 2002 (33), pp. 286 ff.
- Brenkert, George G.: *Marketing Ethics*. Blackwell Publishing 2008.
- Business Week*, "Special Report: White-Collar Crime: Who does the Time?" February 6, 2006.
- Crane, Andrew, and Dirk Matten: *Business Ethics – A European Perspective*. Oxford 2004.
- Denzin, N.K. and K. Erikson: "On the Ethics of Disguised Observation: An Exchange. In: Martin Bulmer (ed.): *Social Research Ethics*, pp. 142 – 151. New York 1982
- Di Norica, V.: *The Knowledge Economy and Moral Community*. In: *Journal of Business Ethics* 2002 (Vol. 38), pp. 167 – 177.
- EMC (European Marketing Confederation). *Code of Conduct*, issued February 2005; retrievable from www.emc.be/codeconduct.cfm
- Ferrell, O.C., J. Fraedrich and L. Ferrell: *Business Ethics. Ethical Decision Making and Cases*. 7th. ed., Boston - New York 2006.
- Financial Times*, 31. Aug. 2001: "P&G admits spying on Unilever".
- Fukuyama, Y. F.: *Trust. The Social Virtues and the Creation of Prosperity*. London 1995.
- Gibson, K.: *Ethics and Business. An Introduction*. Cambridge University Press 2007.
- Gow, D.: *Siemens chairman appeals for leniency from US authorities over bribery scandal*. *The Guardian*, Jan. 24, 2007. (www.guardian.co.uk/business/2008/jan/24/eur ope - 56k).
- Haase, Michaela: "Theory, Practice and Education – On the Role of Business Ethics for Management Education at Business Schools or Universities". In: Cowton, Christopher, and Michaela Haase (eds.): *Trends in Business and Economic Ethics*. Heidelberg 2008, pp. 229 – 261.
- Habermas, J.: *The Inclusion of the Other. Studies in Political Theory*. Cambridge, MA, 1999.
- Harzing, Anne-Wil K., "Managing the Multinationals. An International Study of Control Mechanisms". Edward Elgar 1999.
- Hasson, J., "Telecom troubles." In: *Federal Computer Week*. 16(29), 2002, p. 20-24
- Hayek, F. A. von, „*The Road to Serfdom*" University of Chicago Press, 1994.
- HBR (Harvard Business Review): *Harvard Business Review on Corporate Ethics*, 2003.
- Hefendehl, R.: *Corporate Criminal Liability. Model Penal Code Section 2.07 and the Development in Western Legal Systems*. [http://www.wings.buffalo.edu/law/bclc/bclrarticles/4\(1\)/hefehndehlpdf.pdf](http://www.wings.buffalo.edu/law/bclc/bclrarticles/4(1)/hefehndehlpdf.pdf).
- Hewitt-Dundas, Nola, "Corporate Flexibility. A Comparative Analysis of Small Firms in Northern Ireland and Massachusetts". Avebury, 1997.
- Hofstede, Geert, "Whatever Happened to Masculinity and Femininity?" In: *Cross-Cultural Psychology Bulletin*, 2000 (34), No. 4, pp. 14 – 19.
- IBM (www.ibm.com): *Big Blue Goes Green* (<http://www.ibm.com/systems/virtualization/vie/w/071807.html>)

¹⁰¹ Sims 2003

¹⁰² Ulrich 2008

- Kotler, Philip: *Marketing Management. The Millennium Edition*. Prentice Hall 2000.
- Lenz, Hansrudi: "Why Act Morally? Economic and Philosophical Reasons". In: Cowton, Christopher, and Michaela Haase (eds.): *Trends in Business and Economic Ethics*. Heidelberg 2008, pp. 131 – 152.
- Melloan, George, "Europe's Printemps of Discontent". In: *The Wall Street Journal*, May 31, 2005.
- Mitchell, Charles: *International Business Ethics. Combining Ethics and Profits in Global Business*. World Trade Press 2003.
- MRS (Market Research Society) Code of Conduct (<http://www.mrs.org.uk/standards/codeconduct.htm>)
- OECD (Organization for Economic Cooperation and Development): *Economic Outlook No.79*, June 2006, Annex table 25.
- Palmeri, C., "Guilty Verdicts for Enron Staff," *Business Week*, May 25, 2006.
- Peterson, Richard B., ed., "Managers and National Culture". A Global Perspective. Quorum Books 1993. PR Newswire, "CED Releases Recommendations for Improving Corporate Governance," New York, March 21, 2006.
- Preuss, L.: "In dirty chains? Purchasing and greener manufacturing". In: *Journal of Business Ethics*, Vol. 34 (2001), pp. 345 – 359.
- Ravlin, Elisabeth C., David C. Thomas and Arzu Ilsev, "Beliefs about Values, Status, and Legitimacy in Multicultural Groups – Influences on Intragroup Conflict." In: P. Christopher Early and Harbir Singh (eds.), "Innovations in International and Cross-Cultural Management". Sage, 2000.
- Rawls, John, "Political Liberalism", Columbia University Press, 1993.
- Roberts, R., "Ethics and corporate responsibility following Enron." A presentation to the 2002 annual fall compliance conference: Risk Management for the Real World! Sponsored by National Regulatory Service, September 12, La Jolla, Ca.
- Sarbanes-Oxley Act of 2002. 107th Congress, Public Law 107-204, July 30, 2002.
- Schwartz, S. H., "Beyond Individualism and Collectivism. New Cultural Dimensions of Values". In: U. Kim, H.C. Triandis et al. (eds.): "Individualism and collectivism. Theory, method and application". Sage 1994.
- Seattle Post, Nov. 16, 2007: "Boeing bosses spy on workers"; retrievable from http://seattlepi.nwsource.com/business/339881_boeingsurveillance16.html.
- Sims, Ronald R.,: *Ethics and Corporate Social Responsibility: Why Giants Fall*. Westport 2003.
- Smith, P. B. et al., "National culture and managerial values. A dimensional analysis across 43 nations". In: *Journal of Cross-Cultural Psychology*, 1996 (27), pp. 231 – 264.
- SAI (Social Accountability International): *Social Accountability Standard SA 8000*, updated 2002.
- The Daily Telegraph, 02. Aug. 2001: "Suddens quits as chief of Wm Baird".
- The Independent, 1. Oct. 2002: "Echostar begins piracy lawsuit against NDS".
- Time Magazine, Dec 22, 2002: "Persons of the Year".
- Treviño, Linda K., and Katherine A. Nelson: *Managing Business Ethics. Straight Talk about How to Do It Right*. 3rd ed., John Wiley & Sons 2004.
- Ulrich, Peter: *Integrative Economic Ethics. Foundations of a Civilized Market Economy*. Cambridge University Press, 2008.
- Verschoor, Curtis, "Tyco: An Ethical Metamorphosis". In: *Strategic Finance*, April 2006, Vol.87(10), pp15-16.
- Web-Services:
www.consumerfraudreporting.org
www.corporateregister.com
www.globalreporting.org
- Website Sources:
www.aflcio.org/corporatetwatch/paywatch: „2008 Executive PayWatch"
www.boingboing.net/2006/07/05/coke-employees-buste.html: „Coke employees busted for trying to sell formula to Pepsi"
www.unwiredview.com/2008/05/26/deutsche-telekom-admits-to-spying
- Yukl, Gary A., "Leadership in Organizations". 3rd ed., Prentice Hall, 1994.

Noëmi Manders-Huits and Michael Zimmer:

Values and Pragmatic Action: The Challenges of Introducing Ethical Intelligence in Technical Design Communities

Abstract:

Various Value-Conscious Design frameworks have recently emerged to introduce moral and ethical intelligence into business and technical design contexts, with the goal of proactively influencing the design of technologies to account for moral and ethical values during the conception and design process. Two attempts to insert ethical intelligence into technical design communities to influence the design of technologies in ethical- and value-conscious ways are described, revealing discouraging results. Learning from these failed attempts, the article identifies three key challenges of pragmatic engagement with technical design communities: (1) confronting competing values; (2) identifying the role of the values advocate; and (3) the justification of a value framework. Addressing these challenges must become a priority if one is to be successful in pragmatically engaging with real-world business and design contexts to bring moral and ethical intelligence to bear in the design of emerging information and communication technologies.

Agenda

Implementing Value-Conscious Design: Successes and Disappointments	38
Vehicle Safety Communication Technology	39
User Profiling Infrastructures	40
Summary	40
Key Challenges of Value-Conscious Design	41
Justification of Value Framework	41
Role of the Values Advocate.....	42
Confronting Competing Values	42
Conclusion	43

Author(s):

Noëmi Manders-Huits:

- Organization and contact address: Philosophy Section, Delft University of Technology, PO Box 5015, 2600 GA Delft, The Netherlands
- Telephone, email and personal homepage: ☎ +31 (0)15 278 1788 , ✉ N.L.J.L.Manders-Huits@tudelft.nl, 🌐 www.ethicsandtechnology.eu/index.php/persons/detail/83/

Michael Zimmer:

- Organization and contact address: School of Information Studies, University of Wisconsin-Milwaukee, 576 Bolton Hall, 3210 N. Maryland Ave, Milwaukee, WI 53211, USA
- ☎ 414-229-3627, ✉ zimmerm@uwm.edu, 🌐 www.michaelzimmer.org

Advances in the power and ubiquity of information and communication technologies (ICT) has led to an explosion in new technological tools and services that have become the backbone of our contemporary information society. The inclusion of companies like Microsoft, Google, Apple, and Amazon in the S&P 500 reveal the importance of ICT to our global economy. Success in this competitive business environment often comes to the ICT developer with the best business intelligence, most-skilled designers, and fastest deployment. Yet, the rapid speed of technological evolution and adoption often leaves little time for designers, managers, and other major stakeholders to anticipate and absorb the moral and ethical dimension of the ICTs they deploy. Lacking the time for lengthy reflection, technology companies are often forced to make hurried engineering and design choices that carry moral and ethical consequences.

While concern over the moral and ethical consequences of our modern technological era has existed for some time (see, for example, Friedman, 1997; Johnson & Nissenbaum, 1995; Moor, 1985; Nissenbaum, 2001; Shrader-Frechette & Westra, 1997), recent focus has been placed on how to develop pragmatic frameworks ensure that particular attention to moral and ethical values becomes an integral part of the conception, design, and development of ICT. These include innovative proposals such as Design for Values (Camp, n.d.), Values at Play (Flanagan, Howe, & Nissenbaum, 2005; Flanagan, Howe, & Nissenbaum, 2008), and Value Sensitive Design (Friedman, 1999; Friedman, Kahn, & Borning, 2002). Each of these frameworks – which we will refer to collectively as Value-Conscious Design – seek to broaden the criteria for judging the quality of technological systems to include the advancement of moral and human values, and to proactively influence the design of technologies to account for such values during the conception and design process. In other words, the goal of Value-Conscious Design is to bring moral and ethical intelligence into conversation with existing business and technical intelligence to inform and guide the design of emerging information and communication technologies.

We, the authors, have been involved in two separate attempts to engage with business and technical design communities to influence the design of emerging technological systems in ethical- and value-conscious ways. Unfortunately, the results were discouraging. Drawing from our interventions with business and technical design communities, this article will identify three key challenges of pragmatic

engagement with technical design communities: (1) confronting competing values; (2) identifying the role of the values advocate; and (3) the justification of a value framework. Addressing these challenges must become a priority if one is to be successful in pragmatically engaging with real-world business and design contexts to bring moral and ethical intelligence to bear in the design of emerging information and communication technologies.¹⁰³

Implementing Value-Conscious Design: Successes and Disappointments

The researchers who have championed the various Value-Conscious Design frameworks have enjoyed success in bringing moral and ethical intelligence to bear in the design of technologies, including the development of web browser cookie management tools in support of the values of informed consent and user privacy (Friedman, Howe, & Felten, 2002), the embedding the value of trust in web browser tools to protect Internet users from consumer fraud and identity theft (Camp, 2006; Camp, Friedman, & Genkina, n.d.), the construction of a computer game environment for teaching middle-school girls programming skills to help counter gender inequity in math and computer science while also embodying values such as cooperation, creativity, privacy and

¹⁰³ This article was inspired by the Values In Design Graduate Student Workshop held at Santa Clara University in August 2005. The authors would like to thank Geoffrey Bowker, Helen Nissenbaum, and the other workshop participants for stimulating the discussions that prompted the writing of this article. The authors also thank the faculty and students at the Department of Philosophy and the History of Technology at the Royal Institute of Technology, Stockholm, Sweden, the Center for Philosophy of Technology and Engineering Science at the University of Twente, Enschede, The Netherlands, the Philosophy Section at the Delft University of Technology, Delft, The Netherlands, as well as the attendees of the 2007 Computer Ethics: Philosophical Enquiry conference for their valuable feedback. Particular thanks to Helen Nissenbaum and Sabine Roeser for their thoughtful comments on earlier drafts of this article. This research was sponsored, in part, by an NSF Dissertation Grant (SES-0620772) and a travel grant provided by the Netherlands Organisation for Scientific Research (NWO, R 22-403).

independence (Flanagan et al., 2005; Flanagan et al., 2008), and the creation of a web browser extension to help obfuscate one's web search history records to prevent profiling by search engine providers, fostering the values of privacy and user autonomy (Howe & Nissenbaum, 2006). These cases reveal the promise of influencing the design of new information and communication technologies in order to account for moral and ethical values.

Encouraged by these successful implementations of the Value-Conscious Design framework, we, the authors, were optimistic as we engaged with the technical design communities of two emerging technological systems, aiming to introduce moral and ethical intelligence into their respective design spheres. Zimmer sought to ensure that the value of privacy became a constitutive part of the technological design of emerging networked vehicle safety communication (VSC) technologies in the United States, while Manders-Huits was part of a team of academics specializing in ethics of information technology who participated in a project to create a User Profiling Infrastructure in The Netherlands.

Vehicle Safety Communication Technology

Recent advances in wireless technologies have led to the development of intelligent, in-vehicle safety applications designed to share information about the actions of nearby vehicles, potential road hazards, and ultimately predict dangerous scenarios or imminent collisions. These vehicle safety communication (VSC) technologies rely on the creation of autonomous, self-organizing, wireless communication networks connecting vehicles with roadside infrastructure and with each other. In these networks, both vehicles and infrastructure collect local data from their immediate surroundings, process this information and exchange it with other networked vehicles to provide real-time safety information about the immediate surroundings. Data messages, which are automatically and continuously transmitted from the vehicle 10 times per second, potentially include the vehicle's location, time and date stamps, vehicle speed & telemetry data, and a vehicle identifier. To help facilitate the development and implementation of VSC applications, seven major auto manufacturers, in cooperation with the U.S. Department of Transportation, have formed a joint research program called the Vehicle Safety Communications Consortium (VSCC), with deployment of VSC

technologies forecasted to occur between 2010 and 2016.¹⁰⁴

Coupled with the predicted safety benefits of VSC applications, however, is a potential rise in the ability to surveil a driver engaging in her everyday activities on the roads and highways. VSC technologies potentially enable the collection of information on where drivers go, when they made their trips, and what routes they used. They represent a shift from drivers sharing only general and visually-observable information to the widespread and constant broadcasting of precise, digital information about their daily activities (Zimmer, 2005). The potential integration of VSC technologies into our daily activities on the public roads threatens to foster a scenario where we might be "driving into the panopticon" (Reiman, 1995) of widespread surveillance, and the potential erosion of the values of privacy and autonomy as we drive along the roads.

Since VSC technologies and their related technical protocols and communication standards are still in the developmental stage, Zimmer, with support from the PORTIA project,¹⁰⁵ took the opportunity to apply Value-Conscious Design principles in an attempt to influence the design of VSC technologies so that the value of privacy would become a constitutive part of the design process. Zimmer interacted with VSC project managers and engineers, was given access to technical white papers, and distributed his findings regarding the potential privacy and surveillance threats of VSC technologies. Unfortunately, the results of his engagement with the VSC design community were discouraging. Zimmer's efforts were met with skepticism: some designers viewed that the security gained through data encryption as a sufficient means of protecting user privacy, while others disregarded the threat to privacy altogether. Some potential privacy-protecting encryption solutions (see, for example, Boneh, Boyen, & Shacham, 2004) were rejected, apparently due to concerns over efficiency and costs

¹⁰⁴ For more information see U.S. Department of Transportation (2005), and Vehicle Safety Communications Consortium.

¹⁰⁵ The PORTIA project is a five-year, multi-institutional, multi-disciplinary, multi-modal investigation funded by the National Science Foundation in the Information Technology Research (ITR) program. For more information, see <http://crypto.stanford.edu/portia/>.

outweighing the privacy protections gained. Opportunities to engage further with the design community to address user privacy were hindered, as scheduled “privacy workshops” were cancelled by working groups, while changing personnel and legal concerns stymied sustained collaboration with more sympathetic designers.

In total, while the introduction of new moral and ethical intelligence into the design sphere for VSC technologies brought some increased awareness of the related privacy concerns, full and direct engagement with this design community to achieve the Value-Conscious Design of these emerging technologies remained limited.

User Profiling Infrastructures

Online organizations are increasingly collecting data on users browsing and purchasing habits in order to create detailed user profiles, providing the tools to predict user behavior and provide personalized products and services. For example, online bookstores track and collect information about users’ browsing and purchase history on their sites, resulting in the creation of detailed user profiles which allow the site to provide personalized purchase recommendations. Alongside this growing reliance on user profiles is the desire to be able to build, share and transfer profiles across various systems and platforms – the creation of a widespread User Profiling Infrastructure. For example, the user profile created on the online bookstore could also be shared with a different organization, like a movie rental company, to help predict what kind of movies the customer might want to watch. Similarly, a third party might be able to use a user Profiling Infrastructure to collect information on users’ actions across various systems, such as a law enforcement agency monitoring purchasing habits across various websites in order to predict illegal activity.

While potentially useful, the cross-domain user profiling enabled by a User Profiling Infrastructure is fraught with value and ethical considerations, such as trust, informed consent, privacy and control over the flow of one’s personal information. Recognizing the importance of addressing these value and ethical concerns, a team of academics specializing in ethics of information technology was invited to join the technical design team to help inform the development of such an architecture. As part of this team, Manders-Huits participated in design meetings and discussions, did research in relevant ethical literature, and identified critical points for intervention to ensure that the User Profiling Infrastructure

under consideration protect user privacy and other ethical concerns.¹⁰⁶ Overall, there was a concerted effort to introduce moral and ethical intelligence into the business and technical design environment in order to engage in the Value-Conscious Design of this emerging technical system.

This effort turned out to be more challenging than expected. While the technical designers were confronted with the challenges of the novel research field of ethics and technology, the ethicists found it equally challenging to apply ethical principles to the novelty and uncertainty of a still-emerging technical infrastructure. It was especially difficult to properly explicate and translate ethical considerations to workable requirements and specifications for the other project participants actually building the system. In other words, it proved difficult to operationalize the values so they could be put into the technical design. More discouraging, however, was the insertion of a new project management team who didn’t share the same commitment to value-conscious design or an appreciation for the demands such efforts bring to the design process. When it came time to speed up the progress of the overall project, eliminating (what were perceived as) the complex and time-consuming ethical concerns seemed the easiest route to get the project back on schedule. As a result, the introduction of moral and ethical intelligence was ultimately rejected.

Summary

While some of the original framers of the Value-Conscious Design (VCD) frameworks have enjoyed success in designing technologies that sustain moral and ethical values, the attempts by Manders-Huits and Zimmer were disappointing and failed to achieve the desired results. One key difference between the successful introduction of moral and ethical intelligence into business and technical design contexts by the original framers of VCD, and the less-successful efforts by the authors, is the particular sites of engagement. The successful applications of Value-Conscious Design principles noted above share a common characteristic of being situated in the relatively non-hostile design environment of the academic laboratory. Each project’s design team was, by and large, comprised entirely of academics committed to the goal of achieving

¹⁰⁶ For more information, see https://doc.telin.nl/dscqi/ds.py/Get/File-52040/TUD_sotas.pdf

Value-Conscious Design, creating a design context quite welcoming of each projects' goals.

In contrast, Manders-Huits and Zimmer attempted to take the principles of Value-Conscious Design outside the laboratory and engage directly with designers of emerging technical systems in their native environments, revealing unique challenges that must be addressed in order to successfully introduce moral and ethical intelligence into "real-world" business and technical design environments outside the walls of academia.

Key Challenges of Value-Conscious Design

The unsatisfactory attempts to engage in Value-Conscious Design detailed above illuminate three key challenges that must be addressed before these pragmatic frameworks can be fully and successfully deployed in design contexts outside the academic laboratory: (1) the justification of a value framework, (2) identifying the role of a values advocate, and (3) confronting competing values. Attention to each of these challenges is critical to ensure moral and ethical intelligence can enter into business and technical design environments.

Justification of Value Framework

It is important to identify whose moral framework we are considering in each specific design setting. The challenge is to identify the extent or limits of the design community: Is it composed only of the actual technology designers, e.g. the engineers, or including contractors, managers, companies, potential customers, etc.? In other words, 'whose' moral framework are we to study? After the identification of the design community and their values – as far as these are tangible – an important step can be taken with respect to value choices in the design process.

The aim of the specific value conscious design project also needs to be framed in terms of the normative stance one wishes to take. One might prefer an 'organic, emergent' moral framework to justify the value choices to be encountered, or have a more specific and predetermined moral framework in mind, driven by a specific normative outlook. Either way the starting point for moral evaluation needs to be clarified so that it is clear what is to be expected with regard to the value commitments of the technology. Accordingly, the design process of the particular technology can be structured accord-

ing to certain points of intervention with respect to value choices.

Friedman and her collaborators (Friedman et al., 2002) argue with respect to universal and particular values that a value sensitive design should be flexible with respect to local values. A practical illustration of this is provided by the RAPUNSEL project (Flanagan et al., 2005). In this computer gaming design, players are tempted to take on part of the design of the game by choosing any particular set of preferences or normative outlook before entering into the game. A potential participant finds herself forced to choose between certain physical attributes, gender, race, etc. before entering the game. As she may not be comfortable with regard to any of these pre-designed categories, the designers allow significant flexibility to add nuances to the character. This flexible design feature, however, is easily provided from the safe settings of the academic gaming environment and we wonder, referring back, if this flexibility is equally manageable outside of these settings. Economic interests might constrain the number of options made available in a commercial gaming environment, and any such limitations present artificially simplify the complexity of moral life.

The justification of (pre-)determined value choices during design demands clarification of the moral framework being used with respect to freedom from bias, autonomy, privacy, equity and other human values. Moreover, it calls for a different way of doing ethics. Where traditionally, ethics is a field where past events are discussed and evaluated in order to develop a comprehensive account of moral choices and phenomena, what is required for a successful implementation of moral theory and values into design, is the "frontloading of ethics" (Van Den Hoven, 2005), also referred to as the changing of a retroactive to a proactive application of ethics. This is a challenging enterprise. Since technology design cases are fundamentally uncertain and with complex future outcomes, it is difficult from an ethical perspective to provide a useful account for dealing with value choices. It demands a revolution in ethics where traditional accounts are reconsidered in light of the complexity of technological design. An important first step in the frontloading of ethics is establishing the role of a values advocate on technical design teams. However, as the next section will detail, this is often a complicated and contentious task.

Role of the Values Advocate

It is the challenge for the values advocate to support all value choices with the necessary normative justification. The acceptance of the values advocate in the design team as holder of particular expertise is dependent on the perception that the value choices and positions held by the advocate are rationally and theoretically justified. We think all choices in the design process have moral import. It is the task of the values advocate to make these as explicit as possible. In some cases the values advocate may also need to justify his or her own presence in the design team, and why designers, or anyone for that matter, should be concerned with values of moral import in the first place.

Further, we envision an array of roles that the values advocate can take within a particular design context: the authoritarian role, the supporting role or the leadership role. In the first role, the values advocate is regarded as authoritative in the ethical and value considerations at hand, implementing value-conscious decisions using a top-down strategy. Such a role is often confrontational, where pressure is exerted (both internally and externally) to ensure proper attention to values. A second role, the supporting role, is a comparatively passive accompaniment of the design process, raising awareness at moments where value choices are being made and pointing to possible alternatives without advocating the one or the other. An advocate in this role is often merely advisory, and might have little more than token input on design decisions. Finally, the leadership role enables the values advocate to be both supporting but also directing when it comes to value choices. By providing insight to the complexity and delicacy of value choices basing on theoretical knowledge as well as acquired practical expertise, the values advocate in her role as leader is able to educate the other members of the design team (and possibly other stakeholders) and to strongly promote certain choices over others where necessary. We argue the leadership role to be the preferred positioning of the values advocate within a design team, taking into account shared responsibility for value choices (whereas the first example of an authoritative role might be too heavy-handed) and a proactive stance of the values advocate (whereas the example of a supporting role might be too passive).

Confronting Competing Values

Perhaps the most apparent challenge of engaging in Value-Conscious Design outside the academic labor-

atory is the inevitability of confronting competing values within varied design contexts. Rather than benefiting from working within the academic sphere committed to the primacy of designing for moral values, design contexts outside academia often include stakeholders whose goals might come into conflict with the protection of these values.

For example, Howe and Nissenbaum's TrackMeNot web browser extension was developed using Mozilla's open-source browser application framework and posted to a website for download by the user and development community. As an academic project, little concern was necessary for production or distribution costs, advertising, profits, or other factors typically in play in commercial software development contexts. In contrast, the attempts at pragmatic engagement in design contexts outside academia by Manders-Huits and Zimmer exposed how the pressures of the marketplace – with its focus on instrumental values of efficiency, productivity and profitability – might result in hostility to the privileging of moral values in the design process. As Agre and Harbs (1994) warn, standard-setting processes often "embed a wide variety of political agendas" and the process of developing those standards will be "contested along a variety of fronts by various parties" (p. 84). The same can be said for technical design overall, and engaging in Value-Conscious Design in real-world design contexts will require the ability to negotiate such instances of conflicting values.¹⁰⁷

We claim that, for a fully engaged and pragmatic application of Value Conscious Design to be successful, it must ensure that values are not only discovered and clarified, but also consciously and deliberately built into design, even if such embedding of values conflicts with other design objectives. This questions the supremacy of some values over others (hierarchy of values) and the way value choices in design are dealt with in light of supporting value systems or political/ethical convictions. While some embrace a more cultural constructivist approach where values are taken as perceived by the majority of the people, we take a more normative position. Here, ethics provides (other) grounds for identifying values and arguing for the enclosure or the supre-

¹⁰⁷ To their credit, Flanagan and her colleagues make it clear in their discussion of the RAPUNSEL project that such projects, when pursued purely within academic contexts, fail to "address all factors that, for example, a commercial project would be obliged to address" (Flanagan et al., 2008).

macy of certain values over others, possibly against the (uncritical) majority opinion. We argue that, for morality to be designed into technical systems and institutions, value choices should be based on well-considered ethical judgments, coherent with our attitude towards how we think the world is best served and structured from a moral perspective. This involves a critical attitude towards certain aims of research and design that are often taken for granted, such as maximum efficiency, maximum profitability, and so on.

Conclusion

We have identified three key challenges that must be addressed if scholars committed to Value-Conscious Design are to be successful in pragmatically engaging within business and technical design communities to introduce moral and ethical intelligence into the decision-making matrix. First, we confront the broad philosophical challenge of providing a sufficient justification of the value and moral framework we embrace when engaging in value-conscious design. Second, the role of the values advocate must be both clearly defined and justified to fulfill its role as an essential component of technical design teams. Finally, we must find strategies to successfully resolve the inevitable value conflicts when engaging with design communities outside of academia.

Our goal with this article is not to discredit the accomplishments of the existing Value-Conscious Design efforts, but merely to show that pragmatic challenges remain. Moreover, like many academic probes, this article presents more questions than answers. By bringing focus to these challenges, however, we hope to spark new critical reflection within the Value-Conscious Design community (within which we include ourselves) of how to best engage with real-world design communities to introduce moral and ethical intelligence into business and design contexts. Addressing these challenges will increase the chances for success of future pragmatic engagements with design communities to proactively influence the design of emerging technologies to take account of ethical and human values.

References

- Agre, P. & Harbs, C. (1994). *Social Choice about Privacy: Intelligent Vehicle-highway Systems in the United States*. Information Technology and People, 7(4), 63-90.
- Boneh, D., Boyen, X., & Shacham, H. (2004). *Short group signatures*. Proceedings of Crypto, 4, 41-55.
- Camp, L. J. (2006). *Reliable, Usable Signaling to Defeat Masquerade Attacks*. Retrieved September 23, 2006, from <http://www.ljean.com/files/NetTrustEcon.pdf>
- Camp, L. J. (n.d.). *Design for Values, Design for Trust*. Retrieved September 20, 2006, from <http://www.ljean.com/design.html>
- Camp, L. J., Friedman, A., & Genkina, A. (n.d.). *Embedding Trust via Social Context in Virtual Spaces*. Retrieved September 23, 2006, from <http://www.ljean.com/files/NetTrust.pdf>
- Flanagan, M., Howe, D., & Nissenbaum, H. (2005). *Values at play: Design tradeoffs in socially-oriented game design*. Conference on Human Factors in Computing Systems, 751-760.
- Flanagan, M., Howe, D., & Nissenbaum, H. (2008). *Values in Design: Theory and Practice*. In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy*. Cambridge University Press.
- Friedman, B. (1997). *Human values and the design of computer technology (CSLI lecture notes; no. 72)*. New York: Cambridge University Press.
- Friedman, B. (1999). *Value-Sensitive Design: A Research Agenda for Information Technology*. National Science Foundation, Contract No: SBR-9729633).
- Friedman, B., Howe, D., & Felten, E. (2002). *Informed consent in the Mozilla browser: Implementing value-sensitive design*. Proceedings of the 35th Annual Hawaii International Conference on System Sciences.
- Friedman, B., Kahn, P., & Borning, A. (2002). *Value Sensitive Design: Theory and Methods*. (Technical Report 02-12-01).
- Howe, D. & Nissenbaum, H. (2006). *TrackMeNot*. Retrieved August 27, 2006, from <http://mrl.nyu.edu/~dhowe/TrackMeNot>
- Johnson, D. & Nissenbaum, H. (Eds.). (1995). *Computers, ethics & social values*. Englewood Cliffs, N.J: Prentice Hall.
- Moor, J. (1985). *What is computer ethics?* Metaphilosophy, 16, 266-275.
- Nissenbaum, H. (2001). *How computer systems embody values*. IEEE Computer, 34(3), 118-120.
- Reiman, J. (1995). *Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future*.

Santa Clara Computer and High Technology Law Journal, 11(1), 27-44.

Shrader-Frechette, K. & Westra, L. (Eds.). (1997). Technology and values. Lanham, MD: Rowman & Littlefield.

U.S. Department of Transportation. (2005). Vehicle Infrastructure Integration (VII): Major initiatives. Retrieved December 18, 2005, from http://www.its.dot.gov/vii/vii_overview.htm

Van Den Hoven, M. J. (2005). Design For Values And Values For Design. Information Age, August/September, 4-7.

Vehicle Safety Communications Consortium. (n.d.). Vehicle safety communications project: Task 3 final report: identify intelligent vehicle safety applications enabled by DSRC. (on file with author)

Zimmer, M. (2005). Surveillance, privacy and the ethics of vehicle safety communication technologies. Ethics and Information Technology, 7(4), 201-210.

Edward Howlett Spence:

The Epistemology and Ethics of Media Markets in the Age of Information

Abstract:

The paper will seek to demonstrate that information as communication has a dual inherent normative structure that commits its disseminators, especially the media, offline and online, to epistemological and ethical principles that are universally mandatory. With regard to the dissemination of information by the media, its *business intelligence* constituted by its commercial interests as a *media market* must always be congruent with *moral intelligence* on the basis of the epistemological and ethical universal principles that the dual normative structure of information gives rise and to which the media itself is committed. When the media's business intelligence comes into conflict with moral intelligence, the latter must always take precedent over the former. Moreover, the communication of information to the public by the media, offline and online, even if conceived merely as another *market commodity*, commits the media to ethical conduct regardless of any other commercial interests that may come into conflict with the media's ethical commitments to the public.

Agenda

Introduction.....	46
The Dual-Obligation Information Theory (DOIT)	47
The Normative Structure of Information	47
The Rights of Informational Agents based on Alan Gewirth's Argument for the Principle of Generic Consistency	48
Conclusion.....	50

Author(s):

Edward Howlett Spence:

- Organization and contact address: Department of Philosophy, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands, and The Centre for Applied Philosophy and Public Ethics (CAPPE), LPO Box 8260, ANU Canberra, ACT 2601, Australia
- Telephone, email and personal homepage: ☎ +31 (0) 53 489 2308 (office); + 31 (0) 626 34 38 31, ✉ e.h.spence@utwente.nl

Introduction

In keeping with the theme of this special issue of IRIE, "business intelligence meets moral intelligence", the paper will seek to demonstrate that with regard to the dissemination of information by the media, its "business intelligence" must be congruent with "moral intelligence" and when in conflict moral intelligence on the basis of universal moral principles that the media itself is committed to, must always take precedent over the media's own business intelligence. The communication of information to the public by the media, offline and online, even if conceived merely as another *market commodity*, commits the media to ethical conduct irrespective of any other commercial interests that may come into conflict with the media's ethical commitments to the public. In summary, this is for at least three reasons:

- (1) Information as communication has a *dual inherent normative structure* that of necessity commits its communication by all *informational agents*, including the media especially, to ethical conduct that cannot be avoided or overridden by any other conflicting self-interest, including commercial interests.
- (2) With regard to the dissemination of information in the form of *news*, the media, and especially the media in the form of journalism, is committed moreover, by its own internal professional ethical code, to the fundamental principle that the public has a right to know and be informed on matters of public interest truthfully, in an unbiased, balanced and fair manner¹⁰⁸.

¹⁰⁸ The public's right to know or the public's right to be informed on matters of public interest is a fundamental principle of journalism enshrined in practically all journalistic ethical codes around the world. It is in fact, what gives the media in the form of journalism, its special status as the 4th Estate, a role that allows them "freedom of the press" and other special privileges not shared or allowed to other commercial enterprises, even to the government that has limited powers to what information it can lawfully access and disseminate on matters concerning its citizens. This places the media, at least in the form of journalism, in a special privileged position in the access and dissemination of information to the public. It is a privilege

- (3) Even if information in the form of communication is construed as a marketable commodity subject to the same commercial exploitation as other marketable commodities, the media perceived merely as a commercial enterprise is also bound to ethical conduct. For consider: if information is conceived merely as a marketable commodity, then media-markets have a similar responsibility as the food industry or the pharmaceutical industry, for example; namely, that the production and delivery of those products, generally perceived as *public goods* (*food, medicines, information*), are what they claim to be (their description is true or truthful – for example, meat is real meat and not some "meat-substitute" designed to look like real meat in order to mislead or deceive the consumers). Hence, those public goods are fit for human consumption and meet normative standards both in their production and distribution. Those standards, in turn, are regulated both within and outside those industries for the ultimate protection and good of society. We can, therefore, ask no less of the media, even if we perceive it purely as a commercial enterprise.

In relation to the potential conflict of roles within the media as both public informers and commercial enterprises, the paper will also briefly analyse the specific roles of the different types of the media - in particular, journalism and public relations - in order to show how those roles are epistemologically and ethically inconsistent with each other and moreover how the convergence of those inconsistent media roles is conducive to *media corruption* – that is, the corruption of information communicated to the public. Given financial cut-backs within media organisations, the corporate media increasingly relies on media releases produced by Public Relations practitioners to communicate information to the public. In view of this practice, can the Fourth Estate be trusted to tell people the truth all the time or even some of the time? Should the public adopt a more sceptical attitude towards the media in view of their commercial interests which are not always congruent with their role as information providers?

which can be of great benefit to society as the exposure of the Watergate scandal by the Washington Post's investigative journalists demonstrates, and of great harm when that privilege is abused as in typical cases of media corruption that will be outlined below.

The Dual-Obligation Information Theory (DOIT)

The dual-obligation information theory (DOIT) model comprises two main parts that together seek to demonstrate that information is *doubly normative* (Spence 2007a):

- (A) Information has an inherent normative structure that commits its producers, communicators and users, everyone in fact that deals with information, to certain mandatory epistemological and ethical commitments;
- (B) The negligent or purposeful abuse of information in violation of the epistemological and ethical commitments to which its normative inherent structure gives rise is also a violation of universal rights – specifically, universal rights to freedom and wellbeing to which all agents are entitled by virtue of being agents, and in particular *informational agents*.

Hence, the abuse of information through, for example, misinformation practices, constitutes (a) a violation of the epistemological and ethical commitments to which the inherent normative structure of information gives rise and (b) a violation of universal rights to which all agents and specifically informational agents are entitled.

Echoing Umberto Eco's claim in *The Open Work* (1989, 66) that with regard to human beings information theory becomes communication theory - the paper will show that the demonstrated dual normative structure of information in terms of its own inherent normative structure, as well as the universal rights of informational agents to which it gives rise, confirms and supports Eco's claim.

The Normative Structure of Information

In providing the dual normative model for the evaluation of information outlined above, the paper will employ an epistemological account of information based on a minimal *nuclear* definition of information. Following Luciano Floridi it will define *information* as "well formed meaningful data that is truthful" (2005) and following Fred Dretske it will define information as "an objective commodity capable of yielding knowledge"; knowledge in turn, defined as "information caused belief" (1999, 44-45 and 86).

What is necessary for both information and knowledge is truth. For information without truth is not strictly speaking information but either *misinformation* (the unintentional dissemination of well-formed and meaningful false data) or *disinformation* (the intentional dissemination of false "information"). Of course, journalists, for example, both offline and online cannot always *know* with certainty whether the information they disseminate is true or not. However, in such cases, they should at least have a reasonable justified belief, responsive to at least some minimal objective verification capable of sustaining that belief that the information they disseminate is probably if not certainly true. One could make the case, for example, that the dissemination of "information" by journalists concerning the claim that Iraq possessed weapons of mass destruction before the start of the war in Iraq was not based on a reasonable justified belief capable of yielding knowledge. Insofar as this was the case, the dissemination of such "information" was misinformation at best, disinformation at worst.

How about, however, media reports that merely stated the US government's claims that Iraq had weapons of mass destruction? What is the *informational* status of such media reports, given that information must be true or at least truthful? Insofar as those reports were true (the US government did in fact make those claims as reported by the media) then those media reports qualify as information because true, notwithstanding that the claims themselves were untrue or not known to be true. For the truth that renders those reports *informational* concerns and relates to what the US government claimed and not the truth about the claims themselves. Generally, media reports of the form (Z) = "X claimed Y" would qualify as information so long as it is true that "X claimed Y" even when "Y" is untrue. For the *truth-maker* that renders the statement "X claimed Y" as information refers to *only* what "X claimed about Y" and not to whether "Y" itself is true or false. For the report "Z" only commits itself to the truth of "X claimed Y" and not to the truth of "Y". To see this more clearly, take the statement "X claimed Y although Y is untrue". This statement is perfectly consistent with both it being true that "X claimed Y" (information) but "Y", contrary to the facts, being false (misinformation). This is because the report "Z" that qualifies as true information concerns only "what X said" and not about whether "what X said is true or false". Of course the media, and specifically investigative journalists, have an additional ethical responsibility to enquire into and inform the public, as a matter of public interest, whether in fact what "X claimed

about Y" was true or false. That is, investigative journalist should not only be concerned about what "X said about Y" but also be concerned about "whether Y is true" and report on the truth or falsity of "Y" accordingly.

Finally, on another related topic, media "news", insofar as it is true or truthful, can also be construed and defined as a type of *new information*. So, for example, the statement "Israel invades Gaza" would have qualified as "news" in the form of "new information" when it was reported in newspapers around the world several weeks ago. However, although now it still qualifies as information - because as a matter of reported fact Israel did invade Gaza some weeks ago - it no longer qualifies as "news" as it is now at present archival "old information" and not "new information"¹⁰⁹.

Using the minimal account of information described above, the paper will now develop a *normative account of information*, which demonstrates and describes the generic epistemological and ethical commitments that necessarily arise in the dissemination of information.

Briefly, the argument is as follows: Insofar as information is a type of knowledge (it must be capable of yielding knowledge, one must be able to learn from it) it must comply with the epistemological conditions of knowledge, specifically, that of truth. And insofar as the dissemination of information is based on the justified and rightful expectation among its disseminators and especially its users that such information should meet the minimal condition of truth, then the disseminators of information are committed to certain widely recognized and accepted epistemological criteria. Those epistemic criteria will in the main comprise objectivity as well as the independence, reliability, accuracy and trustworthiness of the *sources* that generate the information. The epistemology of information, in turn, commits its disseminators to certain ethical principles and values, such as honesty, sincerity, truthfulness, trustworthiness and reliability (also epistemological values), and fairness, including justice, which requires the equal distribution of the informational goods to all citizens. Thus in terms of its dissemination, information, *as a process and product of com-*

*munication*¹¹⁰, has an intrinsic normative structure that commits everyone involved in its creation, production, search, communication and consumption to epistemological and ethical norms and these norms being intrinsic to the normative structure of information are rationally unavoidable and thus not merely optional.

The Rights of Informational Agents based on Alan Gewirth's Argument for the Principle of Generic Consistency¹¹¹

Gewirth's main thesis is that every rational agent¹¹², in virtue of engaging in action, is logically committed to accept a supreme moral principle, the Principle of Generic Consistency (PGC). The basis of his thesis is found in his doctrine that action has an inherent normative structure, and because of this structure every rational agent, just in virtue of being an agent, is committed to certain necessary prudential and moral constraints.

Gewirth undertakes to prove his claim that every agent, *qua* agent, is committed to certain prudential and moral constraints in virtue of the inherently normative structure of action in three main stages. First, he undertakes to show that by virtue of engaging in voluntary and purposive action, every agent makes certain implicitly evaluative judgments about the goodness of his purposes, and hence about the necessary goodness of his freedom and

¹¹⁰ This qualifying phrase is used to emphasize that it is only as a process and product of communication that information becomes inherently normative due to the reasonable and rightful expectations that informational agents have with regard to the truthful communication and dissemination of information. That is, we reasonably and rightfully expect and trust that we won't be lied to or misinformed when engaging in inter-informational-communication practices with others.

¹¹¹ A full and detailed analysis and defense of the argument for the PGC against all the major objections raised against it by various philosophers can be found in Spence 2006 (Chapters 1 to 3), Deryck Beylveled (1991) and Alan Gewirth (1978).

¹¹² Understand "rational agent" to mean any putative agent who is minimally capable of inductive and deductive reasoning of the most basic and minimal kind including instrumental reasoning or "means-end reasoning".

¹⁰⁹ I would like to acknowledge my thanks and gratitude to the reviewers of this paper for bringing these additional matters and their relevance concerning the truth condition of information to my attention.

wellbeing, which are the necessary conditions for the fulfillment of his purposes. Secondly, he undertakes to show that by virtue of the necessary goodness which an agent attaches to his freedom and wellbeing, the agent implicitly claims that he has rights to these. At this stage of the argument, these rights being merely self-regarding are only prudential rights.

Thirdly, Gewirth undertakes to show that every agent must claim these rights in virtue of the sufficient reason that he is a *prospective purposive agent* (PPA) who has purposes he wants to fulfill. Furthermore, every agent must accept that, since he has rights to his freedom and wellbeing for the sufficient reason that he is a PPA, he is logically committed, on pain of self-contradiction, to also accept the rational generalization that all PPAs have rights to freedom and wellbeing (Gewirth 1978, 48-128). At this third stage of the argument these rights being not only self-regarding but also other-regarding, are moral rights. The conclusion of Gewirth's argument for the PGC is in fact a generalized statement for the PGC, namely, that all PPAs have universal rights to their freedom and wellbeing.

Applying the PGC to information, we can now make the further argument that information must not be disseminated in ways that violate informational agents' rights to freedom and wellbeing, individually or collectively, (Negative Rights). Moreover, information must as far as possible be disseminated in ways that secure and promote the informational agents' rights to freedom and wellbeing (Positive Rights). Conceived as the Fourth Estate, this places a significant and important responsibility on the media, especially journalists, both offline and online, in their role as disseminators of information to the public.

For example, certain media practices such as *media release journalism* (P. Simmons and E. Spence 2006, 167-181), misleadingly and deceptively disseminate media release information produced by Public Relations professionals as objective and independent information through print or broadcast media sources (newspapers, television and radio) as "news". This occurs without any disclosure that these so called "news stories" are sourced from media releases produced by PR professionals on behalf of their clients, often verbatim and sometimes with the journalists' bylines attached to them. Practices such as media release journalism are therefore ethically objectionable because they are designed to deceive and do deceive the public by stealth, sometimes in

collusion with journalists and government representatives. Moreover, these practices constitute media corruption for they are conducive to the corruption of the informational processes and products that are essential for informing citizens on matters of public interest in an objective, truthful and fair manner¹¹³.

Constrained by space as well as being beyond the scope of this short paper I cannot discuss media corruption in any detail. Suffice to say, media corruption occurs primarily because matters of "business intelligence" at both the individual level of media practitioners as well as at the institutional level of the professional practices of the media organizations themselves are allowed by omission or commission to override matters of "moral intelligence". As we saw above in section (2) matters of moral intelligence with regard to the communication of information by the media must of necessity, both with regard to principle and practice, always override matters of business intelligence when the two come into conflict. Even if we are to construe information purely as a marketable commodity, the media and the market, in principle if not always in practice, can ethically co-exist as in the case of other commercial enterprises that distribute public goods to consumers, such as the food and pharmaceutical industries. Things go ethically wrong, however, when conflicting interests operating within the media become *conducive to media corruption*, such as the example of media release journalism outlined above. For a detailed analysis of a taxonomy of

¹¹³ For a further analysis and discussion of corruption generally and media corruption, specifically, see the following: A. Quinn, and E. Spence. Two Dimensions of Photo Manipulation: Correction and Corruption. Melbourne: *Australian Journal of Professional and Applied Ethics*, 2007; E. Spence. Corruption in the Media, In Jeanette Kennett (Ed.), *Proceedings of GovNet Annual Conference, Contemporary Issues in Governance*, Melbourne, Monash University, Australia, ISBN 0-7326-2287-5, 2005; S. Miller, P. Roberts, and E. Spence. *Corruption and Anti-corruption: An Applied Philosophical Approach*. Upper Saddle River, NJ, Pearson/Prentice Hall, 2005; E. Spence & B. Van Heekeren, *Advertising Ethics*. Upper Saddle River, NJ, Pearson/Prentice Hall, 2005; and E. Spence, A. Alexandra, A. Quinn and A. Dunn (forthcoming 2009) *Media, Markets and Morals*. Oxford: Blackwell Publishers.

media corruption that outlines and examines the different *types* of media corruption see (Spence in press 2008).

Such media corrupt practices, which once appeared only in the old corporate media (newspapers, television and radio), have increasingly become more prevalent on the Internet, for example, in blogs. Media deception is demonstrably unethical on the basis of the PGC because it can actually or potentially at least violate the rights to freedom and wellbeing that people have generally as agents and specifically, as citizens that require accurate, reliable and trustworthy information on matters of public interest. More generally, media deception through collusion by PR professionals, journalists and government representatives, violate all citizens' rights to freedom and wellbeing collectively by undermining the democratic process itself that requires the truthful, fair and objective production and dissemination of information on matters of public interest. It is partly for that reason that media control is sought and exercised by totalitarian regimes, such as those in China and Iran for example, that do not want their citizens to be well informed.

In discussing the link between business intelligence and moral intelligence with regard to information I have specifically focused on the corporate media because it offers a uniquely paradigmatic case of the conceptual and practical convergence between "business intelligence" in the media's role as a type of a commercial market enterprise on the one hand, and "moral intelligence" in its formal role as a professional body of disseminators of public information to citizens and consumers, on the other. However, insofar as information as a process and product of communication necessitates unavoidable epistemological and ethical commitment as demonstrated by the dual-obligation information theory (DOIT) model argued for in this paper, those same commitments apply to all informational agents both inside and outside the media. In particular, it should be emphasized that all informational agents in their functional role within companies (and not just media companies) as well as in their functional role within the market economy generally (for example, for gaining and disseminating information about competitors and products, amongst other things) are constrained by the same epistemological and ethical principles to which the media are committed. This consideration also reveals and renders apparent the important underlying link between media and business intelligence, as most large corporate companies these days have their own internal media departments for disseminating information to the public so

as to protect and promote their business interests¹¹⁴. The widely reported IT fraud in India recently concerning the outsourcing corporation Satyam that has been accused of inflating its profitability status by falsifying its accounts and financial statements, illustrates how terribly things can go wrong both morally and commercially when information is abused and misused to misinform the public, the Stock Exchange, investors, share-holders and clients¹¹⁵. This goes to show that when it comes to information, truth is the best policy, both with regard to business intelligence as well as moral intelligence.

Conclusion

DOIT has provided a meta-conceptual framework comprising two inter-related parts that together demonstrate the epistemological and ethical universal character of information. Together these two inter-related parts have demonstrated the *doubly-normative structure* of information; (a) by disclosing the *inherently normative structure of information* and revealing the epistemological and ethical principles and values inherent in *information as a process of communication* to which all informational agents are universally committed (Spence 2009 in press; and 2007a); and (b) by disclosing the universal rights (freedom and wellbeing) to which all informational agents are entitled by virtue of the *inherent normative structure of action* (Spence 2006; Gewirth 1978; 1996; and Beyleveld 1991). Hence, together these two inter-related parts of DOIT have demonstrated the doubly-normative structure of *information action*, to which all informational agents, including the media are committed by universal necessity. Thus, information as communication can generally be epistemologically and ethically evaluated *internally* by reference to its inherent normative structure. That structure commits its disseminators, to ethical and epistemological norms. This is especially

¹¹⁴ I would like to acknowledge my thanks to the reviewers and editors of this paper for pointing out to me the more general application and relevance of my argument to the business intelligence of companies generally.

¹¹⁵ See, for instance, the article "Indian IT fraud sparks economic fears" by Salil Panchal, reported in the Sydney Morning Herald, January 8, 2009. Accessed on 27/1/2009 on <http://news.smh.com.au/business/indian-it-fraud-sparks-economic-fear-20090108-7c5j.html>

true of the media and its professional communicators such as Journalists and PR Consultants, for example, on-line and off-line.

In addition, the ethical values to which the inherent normative structure of information as communication gives rise requires that the informational agents' rights to freedom and wellbeing must be respected, secured and promoted. Those values are mandated by the Principle of Generic Consistency (PGC) and therefore information can also be *externally* evaluated by reference to the PGC. In sum, *informational action* as both *information* and *action* is doubly normative.

In view if this, the media (including the new media) as the primary producer and disseminator of information to the public through all the different modes and channels of media communication, including journalism, public relations and advertising, offline and online, has a particularly central and crucial moral role in the dissemination of information to the public. This places upon it the highest moral responsibility in ensuring that the information it produces and disseminates accords with the highest epistemological and ethical standards as outlined in this paper, notwithstanding that the media, as media-markets, operating within a free-market economy, is also unavoidably and perhaps desirably, a commercial enterprise. However, as we would not settle for less stringent norms of professional conduct from other commercial industries such as those of the food and pharmaceutical production and distribution industries, we should not be expected to settle for less when it comes to the media. Information is a vital commodity whose integrity is paramount to the wellbeing of individuals and society. The media's role in safeguarding the integrity of information is therefore of the utmost importance in the age of information. Hence, with regard to the dissemination of information by the media, its business intelligence must always be guided and accord to moral intelligence that of universal necessity is mandated by the dual inherent normative structure of information. Moreover, as discussed above, the same epistemological and ethical constraints apply to all informational agents, both within and outside the media, and in particular informational agents whose role within companies of all types and sizes is critical with regard to both the business intelligence as well as the moral intelligence of the information gathered and disseminated by them to the public, their competitors and to all other relevant stake-holders.

References

- Beyleveld, Deryck (1991) *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency*. Chicago: University of Chicago Press.
- Gewirth, Alan (1978) *Reason and Morality*. Chicago: University of Chicago Press.
- Dretske, Fred (1999), *Knowledge and the Flow of Information*. Stanford, CSLI Publications.
- Eco, Umberto (1989), *The Open Work*, translated by Anna Cancogni. Cambridge, MA., Harvard University Press.
- Floridi, Luciano (2005), *Is Semantic Information Meaningful Data? Philosophy and Phenomenological Research*, Vol. LXX, No. 2.
- Miller, S., Roberts, P., & Spence, E. (2005) *Corruption and Anti-corruption: An Applied Philosophical Approach*. Upper Saddle River, NJ, Pearson/Prentice Hall.
- Simmons, P. and Spence, E. *The Practice and Ethics of Media Release Journalism*. *Australian Journalism Review*, volume 28(1), July 2006, pp.167-181.
- Quinn, A. and Spence, E. (2007) *Two Dimensions of Photo Manipulation: Correction and Corruption*. Melbourne: *Australian Journal of Professional and Applied Ethics*.
- Quinn, A., and Spence, E. (2004c) *Manipulation in Photojournalism: Is it Ethical? Is it Corrupt?* In Anne Dunn (ed.) *Proceedings: Annual Conference of the Australian and New Zealand Communication Association*, Sydney: University of Sydney.
- Spence, E. (lead author), Alexandra, A, Quinn, A and Dunn, A. *Media, Markets and Morals*. Oxford: Blackwell Publishers (forthcoming 2009).
- Spence, E. (in press, 2009) *The Epistemology and Ethics of Internet Information*, in a Springer book of selected papers from the International Association of Information Systems (Italian Chapter) itAIS Conference, Paris, 13-14 December, 2008.
- Spence, E. and Quinn, A. (in press 2008), *Information Ethics as a Guide for New Media*. *Journal of Mass Media Ethics*.
- Spence, E. (in press 2008) *Media Corruption*, *International Journal of Applied Philosophy*.
- Spence, E. (2007a) *What's Right and Good about Internet Information? A Universal Model for Evaluating the Cultural Quality of Digital Information*. In Larry Hinman, Philip Brey, Luciano

Floridi, Frances Grodzinsky and Lucas Introna (eds.,) Proceedings of CEPE 2007, The 7th International Conference of Computer Ethics: Philosophical Enquiry, University of San Diego, USA, July 12-14 2007, ISSN 0929-0672.

Spence, E. (2007b) Positive Rights and the Cosmopolitan Community: A Right-Centred Foundations for Global Ethics, Journal of Global Ethics, Volume 3 Issue 02, July/August 2007.

Spence, E. (2006) Ethics Within Reason: A Neo-Gewirthian Approach. Lanham, Lexington Books (a division of Rowman and Littlefield).

Spence, E. (2005) Corruption in the Media. In Jeanette Kennett (Ed.), Contemporary Issues in Governance: Proceedings of the GovNet Annual Conference, Melbourne, Monash University, ISBN 0-7326-2287-5.