The ethics of information transparency

2 authors, including:

Matteo Turilli
Rutgers, The State University of New Jersey
79 PUBLICATIONS   **1,002** CITATIONS

Some of the authors of this publication are also working on these related projects:

Advanced e-Infrastructure and Cloud Computing View project

An Integrated Middleware Framework to Enable Extreme Collaborative Science (AIMES) View project

The ethics of information transparency

Matteo Turilli · Luciano Floridi

Abstract The paper investigates the ethics of information transparency (henceforth transparency). It argues that transparency is not an ethical principle in itself but a pro-ethical condition for enabling or impairing other ethical practices or principles. A new definition of transparency is offered in order to take into account the dynamics of information production and the differences between data and information. It is then argued that the proposed definition provides a better understanding of what sort of information should be disclosed and what sort of information should be used in order to implement and make effective the ethical practices and principles to which an organisation is committed. The concepts of "heterogeneous organisation" and "autonomous computational artefact" are further defined in order to clarify the ethical implications of the technology used in implementing information transparency. It is argued that explicit ethical designs, which describe how ethical principles are embedded into the practice of software design, would represent valuable information that could be disclosed by organisations in order to support their ethical standing.

Keywords Information transparency · Semantic information · Computer ethics · Software design

M. Turilli (✉)
Oxford University Computing Laboratory (OUCL),
University of Oxford, Oxford, UK
e-mail: matteo.turilli@comlab.ox.ac.uk

M. Turilli
Oxford e-Research Centre (OeRC), University of Oxford,
Oxford, UK

M. Turilli · L. Floridi
Information Ethics Group (IEG), University of Oxford,
Oxford, UK

M. Turilli · L. Floridi
Research Group in Philosophy of Information (GPI), University
of Hertfordshire, Hatfield, UK

M. Turilli
Centre for Ethics and Economics and Business,
Universidade Católica Portugueasa, Lisbon, Portugal

L. Floridi
Department of Philosophy, University of Hertfordshire,
Hatfield, UK

Introduction

"Transparency" has at least two different meanings that, unfortunately, are irreconcilable and hence potentially misleading. In the disciplines of information management studies, business ethics and information ethics, "transparency" tends to be used to refer to forms of information *visibility*, which is increased by reducing or eliminating obstacles. In particular, transparency refers to the possibility of accessing information, intentions or behaviours that have been intentionally revealed through a process of disclosure. In the disciplines of computer science and IT studies, however, "transparency" is more likely to refer to a condition of information *invisibility*, such as when an application or computational process is said to be transparent to the user. In this paper, we shall use the term "transparency" only in the former sense, specifically in relation to the choice of which information is to be made accessible to some agents by an information provider.

Not all authors in the area of business and business ethics explicitly use the expression "information transparency". However, it is clear that they usually link the concept of transparency with the process of making

explicitly and openly available (disclosing) some information that can then be exploited by potential users for their decision-making processes. Winkler, for example, stresses how disclosed information is used, by offering a definition of "transparency" in terms of "amount […] of information […] upon which economic agents base their decisions or expectations" (Winkler 2000). Other authors, like Vaccaro, Madsen and DiPiazza, focus on the act of disclosing information, defining "transparency" as a "degree of completeness of information, provided by each company to the market, concerning its business activities" (Vaccaro and Madsen 2006) and as the "obligation to willingly provide to shareholders the information needed to make decisions" (DiPiazza and Eccles 2002).

The previous definitions highlight the fact that, from the perspective of those who gain access to information (e.g. the public, employees or regulatory bodies), transparency depends on factors such as the availability of information, the conditions of its accessibility and how the information, which has been made transparent, may pragmatically or epistemically support the user's decision-making process. Information providers (e.g. companies, organisations or public institutions) shape such factors by choosing which information could or should be disclosed, also according to current legislation, and by deciding in which form information might be most suitably made available. Such choices and decisions depend on evaluating business, legal and ethical constraints and implications.

Considering the ethical implications of disclosing information is a major challenge for information providers. On the one hand, providers have to evaluate the potential ethical or unethical use of disclosed information. For example, facilitating access to electronic medical records may help life-saving research, but may simultaneously expose patients to fraud or a breach of privacy, as their personal information is disclosed. Alternatively considered, information transparency has the potential to show whether the providers are not only abiding by the legal requirements, but also effectively practising the ethical principles to which they are allegedly committed. For example, disclosed information may contain details that publicly indicate whether companies' activities are consistent with principles of equality, fairness, informational privacy, social welfare or environmental care.

The public perception of providers' ethical standings following the disclosure of information may represent, in some cases, a business opportunity. Consider, for example, the case of the so-called ethical, green and socially responsible banks (Harvey 1995; Sparkes 2001). Their business also depends on disclosing information about the ethical principles endorsed for the regulation of the banks' investments, profit margins or customer care. Banks disclose such information to confirm and publicise the banks' ethical

standings and "good" business practice to their potential and current clients.

Clearly, the ethical implications of information transparency can be a double-edged sword for a company, since disclosing ethically sensitive information shows its degree of ethical coherence. When information users perceive ethical standards to be low, the information provider's image and business may be damaged. The international wave of dissent suffered by Shell UK following the well-known environmental case of Brent Spar (Löfstedt and Renn 1997), or the large debate caused by Monsanto and its ethical arguments for the support of genetically modified crops (Gaskell and Bauer 2001; Magretta 1997) are paradigmatic examples of how delicate and exacting the understanding and management of the ethical implications of information transparency can be.

Such implications become even more far-reaching when the level of automation of information management, so pervasive in many companies and institutions, is factored in. The increasing rate of deployment of technologies capable of operating with some degree of autonomy is transforming companies and institutions into *heterogeneous* organisations[1] in which individuals and technological devices amalgamate and contribute to the management of the information flow, performing activities side by side. In these heterogeneous organisations, the production, management, preservation and access of information are processes of critical importance and hence the ethical implications of information transparency become even more challenging.

The rest of this paper focuses on the ethics of information transparency and the problem of what kind of information should be made available by information providers. More specifically, we shall address three correlated questions:

1. What is the ethical nature of information transparency?
2. What information affects the ethical nature of information transparency?
3. What information should be disclosed in order to implement information transparency in heterogeneous organisations?

The ethical nature of information transparency

Information transparency, understood in terms of disclosed information, does not necessarily imply ethical consequences, since the disclosed information may be ethically neutral. Information transparency may not affect ethical

---

[1] For a comprehensive definition of heterogeneous organisations and for a discussion of the ethical implications of designing their computational artefacts see Turilli (2007).

principles and have only ethically unrelated effects, if any effect at all. For example, the user interface of operating systems (e.g. Windows, OSX or Linux) often discloses information about the underlying computational processes without any ethical consequence. Users may be informed whether their interaction with a program is correct, whether they have received new e-mails or whether there are new upgrades to install. Disclosing such information is a design choice, fundamental for functional human–computer interactions, but that need not qualify as an ethical choice.

Another example of information transparency without ethical connotations is provided by the debate about the economical suitability of disclosing information. Lamming et al. (2004) analyse the consequences of bilaterally disclosing sensitive information and tacit knowledge in supply relationships. In this context, the degree of transparency is considered to be the property of a commercial relationship and is evaluated for its commercial importance. Winkler (2000) analyses the role of (information) transparency in monetary policymaking. In his analysis, information disclosure is evaluated, alongside issues of information communication and interpretation, in relation to its ability to affect the efficiency of monetary policies.

Information transparency is not an ethical principle per se, seeing that it can be ethically neutral, but it can easily become an ethically "enabling" or "impairing" factor, that is a pro-ethical condition, when the disclosed information has an impact on ethical principles. Such an impact depends on at least two types of relationship that occur between disclosed information and ethical principles. One is *dependence*: some amount of information is required in order to endorse ethical principles. The other is *regulation*: ethical principles regulate information flow by constraining its access, usage, dissemination and storage (see Fig. 1). Information transparency is ethically enabling when it provides the information necessary for the endorsement of ethical principles (dependence) or (and this might be an inclusive or) when it provides details on how information is constrained (regulation). Conversely, ethical principles can be impaired if false details (misinformation) or inadequate or excessive amounts of information are disclosed.

Accountability, safety, welfare and informed consent are examples of ethical principles that depend on the disclosure of some information in order to be endorsed. The "enabling" role of information transparency for accountability is well described by Mallin, who argues for the necessity of implementing information transparency into corporate governance because otherwise "accountability would not exist in any meaningful way" (Mallin 2002). Analogously, the recall of 13 million Firestone tyres by Ford in 2001 that were prone to spontaneous 'blow-out' (Moll 2003) and the recall of 10 million laptops by several makers because their batteries posed a fire hazard (Ahrens 2006) show how safety
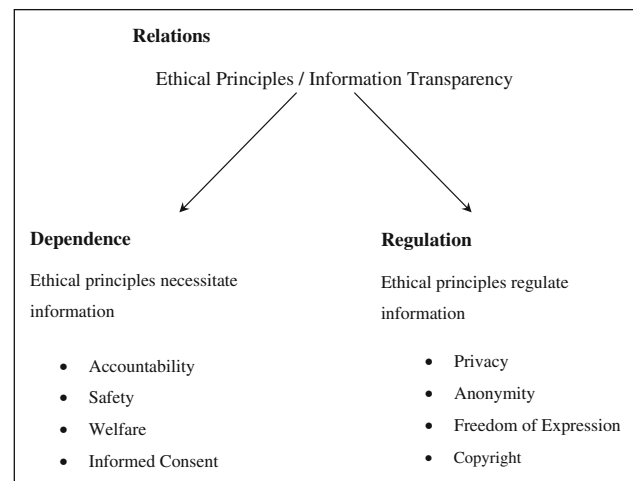

Fig. 1 Relations of dependence and regulation between ethical principles and information. Dependence relation between ethical principles and transparency subsists when ethical principles need to be supported by information. Regulation relation subsists when ethical principles constrain the flow of information

and welfare "enablement" may depend on the disclosure of information to the public.

Privacy, anonymity and copyright[2] are typical examples of ethical principles that regulate the flow of information. Information transparency enables such principles by providing the details of their regulative constraints to the public. Consent forms for the treatment of personal information clarify the extent to which privacy and anonymity will be granted, describing the constraints on access and use of disclosed information. Similarly, details about copyright provide information about how particular information expressed in some form can be copied or used, for example, in derivative work.

Information transparency may impair all of the above ethical principles when false, misleading, partial or inappropriate details are released to the public. Partial details about the management of personal data may impair privacy and anonymity but also generate mistaken beliefs that could further impair accountability or justify a sense of false security or welfare. The financial downfall of Enron/Andersen, Tyco International, WorldCom and Parmalat (Clarke 2007; Coffee 2006), are all infamous examples of how partial information and misinformation disclosed to the public impaired accountability, safety and welfare.

The potential for information transparency to be ethically enabling or impairing poses a general problem concerning the best way to decide what information should be disclosed when ethical consequences are taken into

---

[2] Copyright is here considered as the expression of the ethical principles that inspired the legislators in formulating such a right. For an analysis of the ethical roots of copyright in the United States of America see Warwick (2001).

account. Radical approaches to information transparency—such as full disclosure or completely withholding information relative to the activity of an organisation—merely fail to guarantee positive ethical implications while risking the promotion of negative ones. Unfortunately, there is no easy way to ensure that information transparency is endorsed maximising its ethically enabling characteristics. The information to be disclosed must be carefully considered by evaluating its potential ethical consequences on a case-by-case basis.

Information and the ethical nature of information transparency

The term "information" in "information transparency" is a qualification that indicates *what* is made accessible (that is, "transparent") to the user. The problem of choosing what type of information should be disclosed first requires understanding the characteristics of the entity that is to be disclosed. Information is a term with many meanings, depending on the context in which, and the purposes for which it is used (Floridi 2004). The information disclosed, when implementing information transparency, is supposed to consist of meaningful, veridical, comprehensible, accessible and useful data. This is not a mere litany of properties. This type of information is called semantic information and consists of true[3] semantic content that can be used for epistemic purposes. Semantic information can be pragmatically connected with agents' processes of decision-making (Sequoiah-Grayson, forthcoming) but note that here information is considered from the point of view of agents, companies or organisations that have to disclose information, not of those who have to use it.

Semantic information differs radically from data. A minimal definition of data is "lack of uniformity" (Floridi 2008). A datum is something that 'makes a difference' and, as such, can be perceived, measured and captured via an interaction. Data can be thought of as a precondition for the experience, pre-epistemic entities the existence of which is empirically inferred. Different physical media like books, DVDs or web pages, contain data that can be codified into different formats or languages. Data are, for example, the strings contained in web pages or in databases but also the binary digits obtained through the changes in laser intensity as it interacts with the microscopic indentations of a DVD's surface.

Both data and information are outcomes of elaboration processes. Data may be produced by interactions between physical objects or between agents and the environment. The head of a hard disk produces data when it magnetises a portion of a ferromagnetic plate; researchers produce (raw) data when conducting experiments or observations. Data may also be derived by means of elaborations, as in the case of computations operated by software or when agents add metadata to a database or tag objects such as photographs, video and web sites.

Information is produced through the elaboration of data. Semantic information can be thought of as the result of a set of operations performed by an agent taking raw data as input and producing well-formed, meaningful and truthful data (that is, information) as output (see Fig. 2). Semantic information is not the result of a 'snapshot' or passive observation, but depends on agents' proactive meaningful data elaborations (semanticisation). For example, given a set of data about the performance of financial stock, a broker (agent) can derive the information that a specific set of bank transactions will have to be executed. Analogously, a manager derives information about the overall financial status of her/his company by elaborating on a vast set of data.

The products of semantic elaborations performed by agents over data are informative only if truthful. For example, the results of the elaborations performed by Andersen on the financial data of Enron proved to be uninformative. They were meaningful data, since they were comprehensible, but they did not convey the truth about the factual financial status of the company. On the other hand, veridical business reports about companies' productivity, business plans and, more generally, all the true semantic
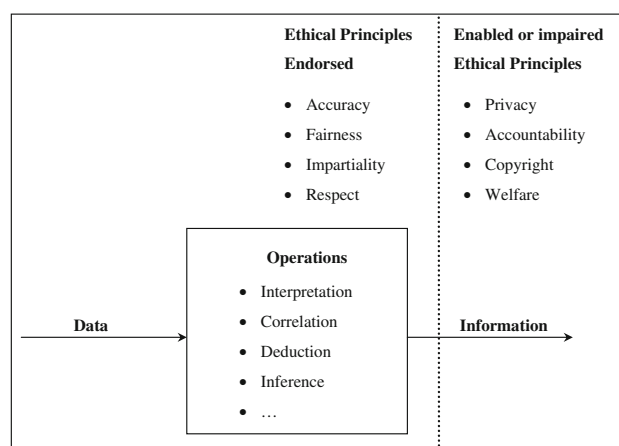
---

[3] For a definite clarification of the need to include truth among the necessary conditions that qualify semantic information see Sequoiah-Grayson (2007). For a review of the debate and an argument in favour of including truth values into the definition of semantic information see Floridi (2007).

Fig. 2 Process of deriving information from data. Data are the input of operations that produce information as output. The ethical nature of information transparency as an ethically enabling (or impairing) feature depends on the set of ethical principles constraining such operations

content that can be properly codified and elaborated about a company, represent factual situations of that company.

As reported in the previous section of the paper, transparency is usually thought of as the process of disclosing a certain amount of information (or data) generated by an organisation. Such information can be codified by means of different media. People outside and/or inside the organisation can access such information and use it for their needs. Ideally, if considered altogether, the disclosed information constitutes a complete picture of the state of the organisation at a given point in time. The problem is that the elaboration processes that have produced such information usually remain opaque.

The elaboration processes of information are not ethically neutral. They are therefore relevant when the ethical implications of transparency are taken into account. Consider, for example, a set of financial statements. When disclosed without explaining how the reported information has been collected, correlated or interpreted, it is all but impossible to understand whether such information is a product of an ethical practise. The same applies to statistical results reported without specifying the methodology that has been used, or the type of analysis that has been applied to the data. It follows that information transparency should disclose not only information but also details about how such information has been produced. Such details are a necessary condition for verifying the consistency between the ethical principles endorsed at the time of producing information and the ethical principles that information transparency should enable. In other words, the possibility of enabling ethical principles by means of information transparency depends on such consistency.

Recall how transparency can enable (or impair) ethical principles (Fig. 1) and consider the schematisation of the production process of information (Fig. 2). The ethical principle of accountability, for example, posits that an agent should be held accountable for the consequences of her/his actions or projects. This principle requires information about the outcome of the agent's actions to be enabled (Fig. 3). Without such information, it would be impossible to evaluate the performance of the agent's actions or projects against qualitative and quantitative parameters. The problem is that neither data (input) nor information (output) is enough for this evaluation. One also needs to know whether such information has been produced while respecting ethical principles of, for example, accuracy and fairness, and whether the semantic content produced is veridical about its subject matter (i.e. agent's actions). Without disclosing the ethical principles endorsed in the elaboration process it is impossible to check whether the ethical principle of, in this case, accountability has been enabled.
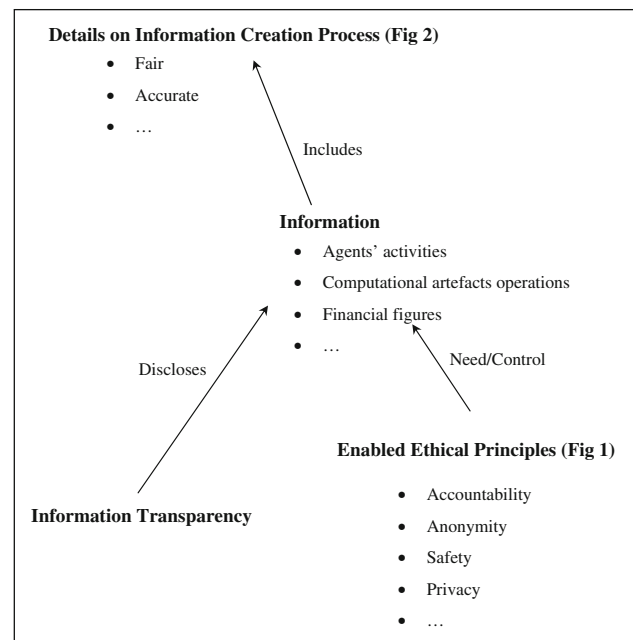

Fig. 3 Schematic generalisation

The same holds true not only for the ethical principles that depend on information (as for accountability) but also for the principles that regulate the information flow. Consider the principle of anonymity and companies that offer anonymising proxies for TCP/IP services, like web surfing, e-mailing and chatting. For these companies, it is crucial to disclose information about how they manage the flow of personal and Internet usage information, in order to prove to their customers that there is no correlation between their identity and their activities online. Disclosing such information requires clarifying whether principles of, for example, fairness or accuracy have been endorsed in its production process. In this example, the principle of anonymity can be "enabled" only on the basis of that clarification.

Again, analogous considerations can be made for those processes that produce data but no information. Such processes take primary/raw data as input and produce further data as output. During these processes, data are codified and correlated. Such operations may have an ethical impact as, for example, in cases of data produced by experiments and observations or when mining, correlating or aggregating data from different databases. All of these operations may be subject to considerations of fairness, accuracy, impartiality or respect and, as such, have to be taken into account when addressing the ethical "enabling" consequences of disclosing a dataset.

The clarification of how the ethical implications of information and data production processes contribute to the ethical impact of disclosed information leads to a shift in the way transparency should be endorsed. The value of

disclosing only ethical or professional codes, recordings or summaries of activities, minutes or meeting reports diminishes when compared to the effects of making transparent also the details about how such information has been produced, elaborated and interpreted. This shift is not surprising once one appreciates that transparency is not an ethical principle in itself. Information transparency, as defined above, is a pro-ethical condition that becomes a valuable tool for uncovering the ethical principles that ideally inspire organisations' decisions and those principles that are factually endorsed in their everyday activities. In this way, organisations, companies or public institutions cannot limit their ethical involvement to public declarations of intent but have to show how the ethical principles, to which they are committed, are prioritised and translated into practise and governance.

Disclosing details about the ethical implications of human choices and actions that compose the process of information production can be achieved by means of accounting or regulatory methods, which may be mandated by legal systems. For example, policies define procedures that allow for reconstructing the employees' behaviour, that indicate what to choose in case of a conflict of interests or whom to refer in case of doubt. The problem is that the management of information is increasingly outsourced to autonomous computational artefacts and it is unclear how their operations relate to ethics. So, the next step is to look at how one may assess the ethical characteristics of the process of information production in the context of heterogeneous organisations, where human and artificial agents are parts of a single, overall system.

Implementing information transparency in heterogeneous organisations

Contemporary organisations usually deploy a vast array of technologies for information management. Such technologies consist of systems for storing, duplicating, validating, communicating and manipulating the flow of digital information. Such systems are composed of man-made objects, such as hardware devices or software products, which here will be referred to as computational artefacts.

Computational artefacts may need human interaction to perform their operations or they may be designed to work with some degree of autonomy. The former are usually deployed in order to augment individuals' capabilities, while individuals tend to outsource some of their activities to the latter. For example, mobile phones and word processors extend users' capabilities for oral and written communication; automated customer support systems, automated trading systems or business process management systems perform some activities instead of human individuals.

Organisations that deploy these types of artefacts become *heterogeneous* as their activities depend upon individuals and computational artefacts and their interactions. Both individuals and computational artefacts simultaneously operate and collaborate with a degree of autonomy in order to achieve the organisations' goals. Financial institutions, public administration, power plants, transportation and defence systems are some obvious examples of large-scale heterogeneous organisations.

Heterogeneous organisations face specific ethical challenges, which have their origins in the digital nature of computational artefacts and their autonomous manipulation of the information flow (Turilli 2007). Digitalisation makes information 'greasier' (Moor 1997) and the flow of information is facilitated in the infosphere by its ontological malleability (Floridi 2006). Large amounts of digital information can not only be easily managed—duplicated, stored, distributed—but can also be mined at an unprecedented speed. Data coming from different sources can be automatically correlated and cross-referenced, thus allowing the rapid derivation of new data and information. Derivation and duplication of information and its global-scale and real time communication represent concrete challenges for the endorsement of ethical principles and rights—privacy, copyright, trust and safety being just some well-known and paradigmatic examples.

Organisations deploy information policies in order to avoid and manage such challenges. Among others, security policies are particularly relevant, as they usually define procedures for authenticating, authorising and accounting for access to, and manipulation of, information. These procedures aim to guarantee that, for example, only a specific set of reliable, legally entitled or trusted people gain access to personal information. In this way, procedures defined by information policies, become an instrument to guarantee that ethical principles are endorsed in organisations' activities.

As argued in the previous section of this paper, details of these procedures should be disclosed when an organisation is committed to enabling a set of ethical principles correlated to information. In the context of heterogeneous organisations, disclosing such details implies the clarification of how both humans and computational artefacts put the relevant procedures into practice. Disclosing only the human implementation portion of such procedures would give a partial coverage of the activity of the organisations and, as a consequence, allow only partial transparency of their ethical implication. However disclosing information about how computational artefacts put procedures into practice requires an evaluation of their design. This evaluation should clarify, for example, what parameters are

used for authorising the manipulation of information, whether information is properly encrypted when transmitted and, more generally, whether all the operations performed by computational artefacts are compatible with the normative constraints of the ethical principles endorsed by an organisation and translated into policies.

This type of design evaluation is problematic because it is unclear how ethics relates to computational artefacts. While it is possible to clarify how ethics can be enforced through policies, and how such policies are translated into procedures, it is problematic to establish a direct link between the computational operations performed by the artefacts and the ethical principles by which those procedures originally transpired. Computational operations are theoretical entities expressed in formal languages that are semantically very distant from the richness of the natural languages in which ethical principles and (the majority of) procedures are expressed.

The problem of embedding ethics into software design is enormous and relates to several disciplines such as software and requirement engineering, law, normative ethics, applied and information/computer ethics and sociology (Friedman et al. 2002; Turilli 2008). From a theoretical standpoint, it is necessary to understand what it means to consider ethics in the context of software engineering. Ultimately, such analysis has to be grounded on phenomenological investigations to facilitate integration into the practice of software design. Alongside such investigations, it is necessary to develop specific formal tools that make it feasible to shift from the informal language, used to investigate ethical requirements, to the formal aspects of software development.

In Turilli (2007) a method has been proposed for the translation of (any arbitrary number of) ethical principles into preconditions for the execution of the artefact's operations. The first step of the proposed translation method is the adoption of descriptive qualitative techniques for eliciting the ethical requirements relevant to the environment in which the computational artefact will be deployed. In the second step, these ethical requirements are translated into a design specification by means of a conceptual tool that has been called 'control closure'. Such a tool can be readily formalised so as to be compatible with the software development practice (Sanders and Turilli 2007).

The method of embedding ethical principles into the practice of software design by means of the control closure uncovers the connection between the operations performed by computational artefacts and the preconditions under which such operations can be performed. Ethical principles relative, for example, to the management of information flow, can be represented by a class of preconditions that constrains the execution of computational operations. Such

preconditions are described at the time of design, thus providing the opportunity to consider the ethical implication of software specification.

This method creates a bridge between ethical principles and the formal details of computational artefacts' behaviours, thus opening the possibility of implementing information transparency in a way that enables a chosen set of ethical principles. Assuming that details of how organisations' activities are performed by both humans and computational artefacts are disclosed, and that such details account for what ethical principles have been factually endorsed in the processes of information production, information transparency can enable the ethical principles to which heterogeneous organisations are committed. For example, disclosing complete details about what ethical principles are respected by computational artefacts in manipulating the information flow of an organisation offers the possibility to be fully accountable, to verify that safety standards are respected or to increase public trust.

Conclusions

In this paper, we have offered two main contributions to the analysis of information transparency. The first consists in a definition of the ethical nature of information transparency, not as ethical principle in itself, but as a pro-ethical condition, that is, an operation that becomes ethically "enabling" when the disclosed information is considered in a relationship of 'dependence' or 'regulation' with ethical principles.

The second contribution concerns the problem of defining what kind of information should be disclosed by an organisation when the ethical nature of information transparency is taken into account. The common understanding of information transparency as the process of disclosing a set of data has been challenged as too limited, in favour of a more inclusive definition that takes into account also the ethical principles factually endorsed in producing information. On the basis of such a definition, we have argued that disclosing not only information but also details of how such information has been produced enables those ethical principles that either depend on information or regulate it.

These two contributions have each been contextualised and explained. In so doing, we have analysed the challenge of implementing the ethical nature of information transparency in the context of heterogeneous organisations. The analysis has led to the conclusion that in many circumstances there may be a real need to disclose the ethical details of any process of information management, including those performed by computational artefacts. A corollary of such analysis has been the clarification of the

necessity of developing methods for understanding the ethical implications of designing computational artefacts.

This paper provides a first step into the investigation of the challenging issue of how information transparency is related to ethics. The problem of assessing the ethical implications of how disclosed information is utilised by individuals in their decision-making processes will be the next stage in this research. It is a stage that will have to wait for a new article in its own right.

References

Ahrens, M. (2006). *Computer and computer peripheral fires with a discussion of batteries*. Quincy, MA: NFPA.

Clarke, T. (2007). *International corporate governance: A comparative approach*. London: Routledge.

Coffee, J. C. (2006). *Gatekeepers: The professions and corporate governance. Clarendon lectures in management studies*. Oxford: Oxford University Press.

DiPiazza, S. A., & Eccles, R. G. (2002). *Building public trust: The future of corporate reporting*. New York: Wiley.

Floridi, L. (2004). Open problems in the philosophy of information. *Metaphilosophy, 35*, 554–582.

Floridi, L. (2006). The ontological interpretation of informational privacy. *Ethics and Information Technology, 7*(4), 185–200.

Floridi, L. (2007). In defence of the veridical nature of semantic information. *European Journal of Analytic Philosophy, 3*(1), 31–41.

Floridi, L. (2008). Data. In W. A. Darity (Ed.), *International encyclopedia of the social sciences*. Detroit: Macmillan.

Friedman, B., Kahn, P. H., & Borning, A. (2002). Value sensitive design: Theory and methods (UW CSE Technical Report 02-12-01). Department of Computer Science and Engineering: Seattle, University of Washington.

Gaskell, G., Bauer, M. W., & Science Museum (Great Britain) (Eds.). (2001). *Biotechnology, 1996–2000: The years of controversy*. London: Science Museum.

Harvey, B. (1995). Ethical banking: The case of the co-operative bank. *Journal of Business Ethics, 14*(12), 1005–1013.

Lamming, R., Caldwell, N., & Harrison, D. (2004). Developing the concept of transparency for use in supply relationships. *British Journal of Management, 15*, 291–302.

Löfstedt, R. E., & Renn, O. (1997). The Brent Spar controversy: An example of risk communication gone wrong. *Risk Analysis, 17*(2), 131–136.

Magretta, J. (1997). Growth through global sustainability. *Harvard Business Review, 75*(1), 78–88.

Mallin, C. (2002). The relationship between corporate governance, transparency and financial disclosure. *Corporate governance, 10*(4), 253.

Moll, R. (2003). Ford motor company and the firestone tyre recall. *Journal of Public Affairs, 3*(3), 200–211.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *SIGCAS Computer and Society, 27*(3), 27–32.

Sanders, J., & Turilli, M. (2007). Dynamics of control. In *TASE 2007* (pp. 440–449).

Sequoiah-Grayson, S. (2007). The metaphilosophy of information. *Minds and Machines, 17*(3), 331–344.

Sequoiah-Grayson, S. (2007). Information gain from inference. In *LogKCA-07, international workshop on logic and philosophy of knowledge, rationality, and action* (pp. 351–368). Donostia-San Sebastian, Spain: The University of Basque Country Press.

Sparkes, R. (2001). Ethical investment: Whose ethics, which investment? *Business Ethics: A European Review, 10*(3), 194–205.

Turilli, M. (2007). Ethical protocols design. *Ethics and Information Technology, 8*, 253–262.

Turilli, M. (2008). Ethics and the practice of software design. In P. Brey, A. Briggle, & K. Waelbers (Eds.), *Current issues in computing and philosophy*. Amsterdam: IOS.

Vaccaro, A., & Madsen, P. (2006). Firm information transparency: Ethical questions in the information age. In *Social informatics: An information society for all? In remembrance of Rob Kling* (pp. 145–156). New York: Springer.

Warwick, S. (2001). Is copyright ethical? An examination of the theories, laws and practices regarding the private the private ownership of intellectual work in the United States. In R. A. Spinello & H. T. Tavani (Eds.), *Readings in cyberethics* (pp. 263–279). Sudbury, MA: Jones and Bartlett.

Winkler, B. (2000). *Which kind of transparency? On the need for clarity in monetary policy-making*. Frankfurt: European Central Bank.