Alternative Model for Information Ethics

1 author:

Sabah Al-Fedaghi

Kuwait University

219 PUBLICATIONS   **700** CITATIONS

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

Project   Conceptual Modeling for Control of a Physical Engineering Plant: A Case Study View project

Project   Thinking in Terms of Flow in Design of Software Systems View project

Alternative Model for Information Ethics

Sabah Al-Fedaghi

Computer Engineering Department
Kuwait University
Kuwait
sabah@alfedaghi.com

Abstract—**Floridi's resource-product-target (RPT) model has been proposed as a unified approach for Information Ethics (IE). RPT can be used to explain and relate the main concepts of IE. It models morally relative acts on information. This paper introduces an enhancement of the RPT model that represents a more complete conceptualization of the "life of information," establishing a firmer foundation for Floridi's objectives in the field of information ethics.**

Keywords-information ethics; model; information processing; information flow

I. INTRODUCTION

Advances in information technology have raised many important ethical issues, including intellectual freedom, access to information, information privacy, and intellectual property. Information ethics (IE) is concerned with these issues. According to Froehlich [12], IE "has evolved over the years into a multi-threaded phenomenon, in part, stimulated by the convergence of many disciplines on issues associated with the Internet." Mathiesen [14] suggests that "information ethics can provide an important conceptual framework with which to understand a multitude of ethical issues that are arising due to new information technologies."

Information ethics does not emphasize specific technologies but concentrates on the fundamental notion of information ([5, 7, 9]). Floridi [9] proposed to base IE on the concept of information as its fundamental phenomenon is recognized to have an intrinsic moral value. He considers IE the philosophical foundation of moral principles that guide problem-solving procedures in computer ethics. According to such a conceptualization of IE, objects are "information objects," and all information objects have inherent moral value. "This information ethics…must be the environmental ethics for the information environment" [10]. Mathiesen [14] (see also Mather [13]) criticized such a theory of IE since "a theory of information ethics will need to specify the relation between persons and information such that information can be of ethical import."

Floridi's [6] unified approach to IE "can help to explain and relate the main senses in which IE has been discussed in the literature" [11] (see also [16]). Floridi also introduced the resource-product-target (RPT) model of morally relative acts on information. The following is a summary of Floridi's [6] description of this model, shown in Figure 1.

A. Information-as-a-resource Ethics

In this view, information is used to make (better) moral decisions about what can and ought to be done in certain given circumstances. A well-informed agent is more likely to do the right thing (Socrates' conception, Rawls' "veil of ignorance"). Wrong behavior is viewed as the outcome of deficient information. Responsibility tends to be directly proportional to the agent's degree of information.

Of course, a lack of information sometimes achieves morally desirable goals, as in the case of protecting anonymity. Information ethics may be described as the study of the moral issues arising from availability, accessibility, and accuracy of informational resources.

B. Information-as-a-product Ethics

Here, the agent produces information about his/her moral actions. Thus, IE may cover moral issues arising, for example, in such contexts as plagiarism, advertising, propaganda, and misinformation (Kant's analysis).
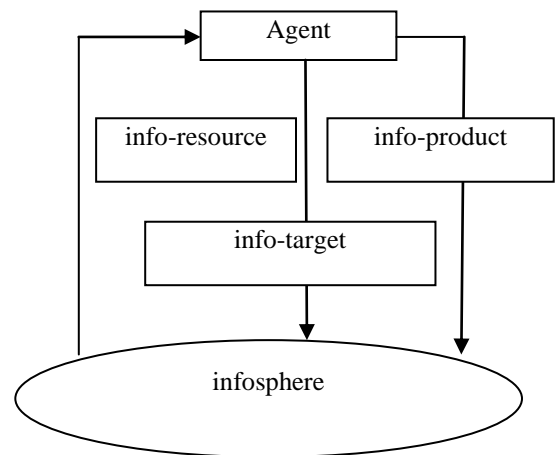

Figure 1 The Resource, Product, Target Model
(From Floridi [6])

C. Information-as-a-target Ethics

Information may be subject to ethical analysis when the agent's actions affect the informational environment, as in such cases as breach of information privacy, hacking, security, and intellectual property.

According to Floridi [6],

> The RPT model … may help one to get some initial orientation in the multiplicity of issues belonging to different interpretations of Information Ethics. The model is also useful to explain why any technology, which radically modifies the "life of information", is going to have profound implications for any moral agent. … At the same time, the model rectifies the excessive emphasis placed on specific technologies …, by concentrating on the more fundamental phenomenon of information in all its variety and long tradition.

Nevertheless, Floridi comments that the model is still too simplistic since several important but different issues are included in analysis of just one "informational arrow." In addition, the model is insufficiently inclusive, since "many important issues…cannot easily be placed on the map at all, for they really emerge from, or supervene on, the interactions among the "informational arrows" [6]. Simply put, the RPT model describes "limited aspects of the information cycle."

In this paper, we introduce an enhancement of the RPT model that describes a more complete conceptualization of the "life of information," thus establishing a firmer foundation for Floridi's objectives in the field of information ethics. The new model, referred to as the information flow model (IFM) will be described in the next section. The remainder of the paper applies this model to information ethics, including a discussion of elimination of weaknesses in the RPT model.

II. INFORMATION FLOW MODEL

The information flow model (IFM) has been proposed and used in several applications [1, 2, 3, 4]. In IFM, the flow of information indicates movement inside and between information spheres. The sphere is the environment of the flow and includes five stages that can have subspheres with their own five-stage schema. Figure 2 shows the state transition diagram of information flow through five states (stages): received, processed, created, released, and transferred.

Information goes through a sequence of states as it moves through stages of its lifecycle, as follows:

1. Information is *received* (i.e., it arrives at a new sphere, similar to passengers arriving at an airport).
2. Information is *processed* without changing its content (i.e., it is subjected to some type of process, e.g., compressed, translated, mined).
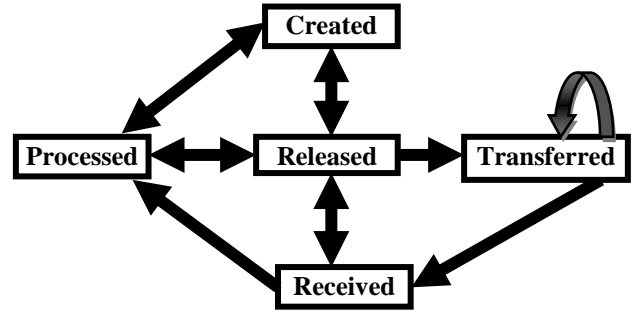

Figure 2. Information states in FM.

3. Information is *released* (i.e., it is designated as released information, ready to move outside the current sphere, such as passengers ready to depart from an airport).
4. Information is *transferred* to another sphere (e.g., from a customer's sphere to a retailer's sphere).
5. Information is *created* (i.e., it is generated as a new piece of information using different methods such as data mining).
6. Information is *used* (i.e., it is utilized in some action, analogous to police rushing to a criminal's hideout after receiving an informant's tip). Using information indicates directing or diverting the information flow to another type of flow such as actions. We call this point a *gateway* in the flow.
7. Information is *stored*. Thus, it remains in a stable state without change until it is brought back to the stream of flow again.
8. Information is *destroyed*.

The first five states of information form the basic stages of the stream of flow. When information is stored, it is in a substate because storage occurs at different stages: information that is created (stored created information), processed (stored processed information), and received (stored received/row information).

Applying the IFM to the RPT model, we observe the following:

- *Information-as-a-resource* in the RPT model is a reference to *received* information by the agent; however, Floridi's category of *Information-as-a-resource* overlooks the fact that "sources" of information can be internal to the agent, as in deducing new information from received information. The agent may conclude that *John is a dangerous man* after receiving outside information about John and comparing it with summary information that categorizes characteristics of dangerous men. Thus, *Information-as-a-resource* can be *created* information in the IFM. According to Floridi [6], "Socrates already argued that a moral agent is naturally interested in gaining as much valuable information as the circumstances require, and that a well-informed agent is

more likely to do the right thing." But Socrates also emphasized analysis of information to *create* knowledge. Thus, *Information-as-a-resource* can be subdivided into received information and created information. This is a significant differentiation in ethics, especially for deciding the responsibilty of the agent in analyzing received information and deducing consequences. For example, an agent suffering from mental illness might *receice* information but with reduced accountability because of inability to *create* conclusions.

- *Information-as-a-product* in the RPT model refers to information *created* by the agent. Here, we observe two types of *Information-as-a-product*:

(a) Created information from received and processed information: In the case of misinformation, a change is made in information, e.g., receiving the information that *John was not at home last night*, then processing it to create the information that *John was at home last night*.

(b) Created information originating from the agent and not based on any previously received information, e.g., the proclamation *I am sent by God*.

Such differentiation has moral significance, as in the case of responsibility toward outside sources of original information, e.g., misrepresentation.

- *Information-as-a-target* in the RPT model refers to processed information in the IFM, but, it may involve other stages of the IFM. Consider the following example from [6]:

> It is not uncommon to mistake it [Information-as-a-target] for a problem to be discussed within the conceptual frame of an ethics of informational resources. This misclassification allows the hacker to defend his position by arguing that no use (let alone misuse) of the accessed information has been made. Yet hacking, properly understood, is a form of breach of privacy. What is in question is not what A [agent] does with the information, which has been accessed without authorization, but what it means for an informational environment to be accessed by A without authorization. So the analysis of hacking belongs to an Info-target Ethics.

In the IFM, this situation can be described as follows:
(a) A hacker without authorization accesses (receives) information without processing it.
(b) A hacker without authorization accesses (receives) and processes information.
Thus, IFM provides fine-grained ethical cases: ethics of receiving information and ethics of receiving information and processing it. It is possible to imagine ethical cases in which information is processed without accessing it, as in a failed attempt to decrypt a message.

III. IFM ETHICS

IFM provides a unified approach for information ethics. As we have shown in the previous section, the RPT model is too coarse to represent the stages of—in Floridi's words—the "life of information." Additionally, the RPT model is incomplete as it ignores combinations of stages (receiving-processing), and the releasing and transferring stages.

Figure 3 is a general view of an "information sphere" (S), including points of information entry into and exit from the system. Unnecessary detail in the IFM is not shown. As shown in the figure, two boundary areas must be controlled:
(1) The boundary for importing information into S is shown by solid circles. Information can "appear" by being transferred from other information spheres, or it can be generated internally (created). Of course, information can be copied at any stage; however, this is not counted as new information in the information sphere.
(2) The boundary for "exporting" (disappearance of) information from S is shown by blank circles. Information can be destroyed at any stage. If several copies exist of information, "disappearance" of information requires erasing all copies.

Accordingly, we can declare different types of information ethics based on the following:
-    Stages
-    Chain of stages
from the appearance of information in the sphere to its disappearance. For example,
-    ethics of perceiving/collecting information
-    ethics of creating information
-    ethics of collecting information, then releasing/ transferring it to outsiders
-    ethics of collecting information processing it, and creating new information (e.g., mining personal information)
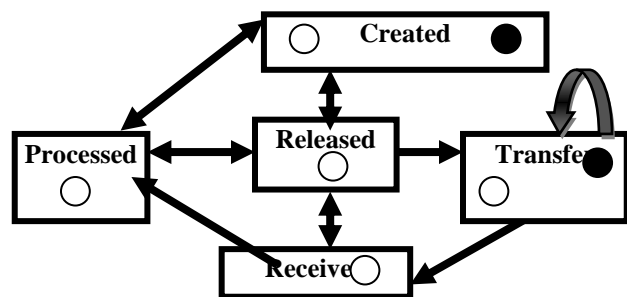

Figure 3. Points of importing/exporting of information.

IV. IFM ETHICS: APPLICATION

IFM can be applied in different areas of information ethics. As an example, consider ACM's Code of Ethics as an outstanding contribution that has promoted ethical practices, as in the case of incorporating ethics codes into the software development decision-making process. Utilizing IFM, we can transform Imperative 1.7 of the ACM code into a more complete and precise system of rules of ethics for handling personal information.

According to Imperative 1.7, "computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals."

The imperative demands taking "precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals." In such a declaration, the reason for emphasizing only accuracy, unauthorized access, and accidental disclosure is unclear. Personal information handling includes many operations, such as gathering, storing, processing, mining, using, disclosing, and transmitting. Breach of personal information privacy can occur at different stages of personal information handling; thus, why not explicitly mention unauthorized collection, use, storage, processing, mining, and creation of personal information? For example, it is possible to illegally process personal information while retaining accuracy and protecting it from unauthorized access or accidental disclosure to inappropriate individuals. The point here is that it is possible to determine, without much elaboration, different manifestations of personal information handling that cover all expected general responsibilities with regard to possible compromise of information privacy.

The ACM imperative implies that "only the necessary amount of personal information be collected in a system." However, what about the amount of personal information necessary for the processing, creating, disclosing, and communicating stages? For example, data mining techniques can produce new personal information that is not collected (e.g., *John A. Smith is a risk*). Why don't we specify explicitly—as in the case of collection—that only the necessary amount of personal information can be mined? The point here is that limits can be specified for all stages of handling of personal information, not just the collection stage.

While it is inevitable that the imperative is subject to some degree of interpretation, it is possible to carefully construct it so as not to burden the computing professionals toward whom the imperative is directed. IFM can be used to elaborate on previous criticisms of the wording of the ACM Code of Ethics, Imperative 1.7.

We propose using the known principles of the fair information practices specified for personal information ethics. We assume that IFM provides the background for the terms and procedures used in the following revision of the imperative.

ACM Code of Ethics, Imperative "1.7 Respect the privacy of others":

It is the responsibility of professionals to adhere to personal information handling ethics. This includes:

- Performing the collecting, processing, creating, releasing, and transferring of personal information by lawful and fair means with the knowledge or consent of its proprietor (Collection Limitation Principle).

- Handling only accurate, complete, and up-to-date personal information that is relevant to its use; and performing only relevant collecting, processing, creating, releasing, and transferring of personal information for its use (Quality Principle).

- Informing the proprietor during any exchange of personal information of the purpose of the recipient obtaining the information. Accordingly, any subsequent handling of the received personal information should be limited to fulfillment of that purpose. Any additional purpose not incompatible with those purposes is specified to the personal information proprietor at each occasion when the purpose is changed (Purpose Specification Principle).

- Not releasing personal information to other agents or declaring at the collecting (receiving) stage, except with the consent of the data subject, or by authority of law (Use Limitation Principle).

- Protecting personal information by reasonable security safeguards against the risks associated with creating, processing, collecting, releasing, and transferring the information (Security Safeguards Principle).

- Adhering to openness regarding development, practices, and policies regarding different stages of personal information handling, including readily available means to establish the existence and nature of personal data and the purposes of their use, as well as the identity and usual residence of the data controller (Openness Principle).

- Respecting the proprietor's right of sovereignty over his/her proprietary personal information on an ongoing basis in order to monitor handling of his/her personal information and take action regarding the welfare of that personal information (Individual Participation Principle).

V. THE ISSUE OF MULTI-INFORMATIONAL ARROWS

According to [6], one weakness of the RPT model is that it is too simplistic. Several issues "belong mainly but not only to the analysis of just one 'informational arrow'." For example, an agent's responsibility may be determined by the information the agent holds, but it may also concern the information the agent issues. Clearly, "holds" refers to stored information in the agent's mind. In IFM, "informational arrows" complement each other. Accordingly, responsibility depends on the chain of flow of information the agent holds, as shown in Figure 4.

(a) Receiving then releasing

(b) Receiving, processing, and then releasing

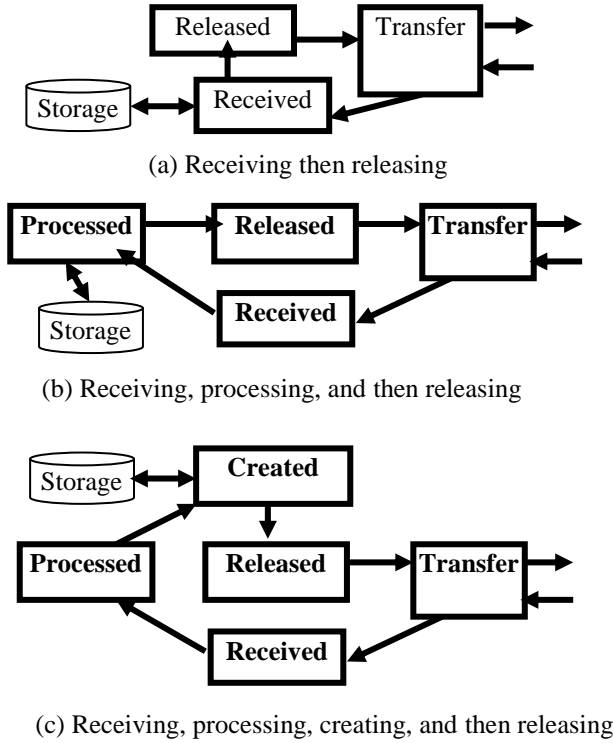(c) Receiving, processing, creating, and then releasing

Figure 4. Responsibility depends on how the agent handles received information.

In (a), the agent receives information, stores (holds) it, and then releases it. For example, the agent receives a message for a third party. Suppose the message is in a language the agent doesn't know. The agent then delivers the message without processing it, e.g., without translating it to understand its content. In computer science this agent is termed a "dump terminal," While the agent is responsible as a messenger, the agent has no responsibility for the content of the message, as in the case of forwarding e-mails in networks.

In (b), the agent receives a message, processes it (e.g., understands its content and translates it), then forwards it to its destination. Clearly, the responsibility here includes the content of the message, as in knowingly delivering child pornography materials.

In (c), the agent receives a message, processes it, accordingly creates information, and then sends it to its destination. In this case, the agent is not only knowingly delivering information, but also actually the creator of information. In a negative example, the agent receives information (e.g., *John visited a shop yesterday*) and then converts it to misinformation (e.g., *John visited a sex shop yesterday*). Accordingly, here the responsibility is different from mere delivery of a message without knowing its content, or knowingly delivering the content of a message.

VI. IFM TRIGGERING MECHANISM

Another weakness of the RPT model is what [6] calls "insufficient inclusiveness." "There are many important issues that cannot easily be placed on the map at all, for they really emerge from, or supervene on, the interactions among the 'informational arrows'. One such example is the 'panopticon' or 'big brother'."

The IFM provides a "triggering" mechanism that can be used in the "panopticon" situation. Simply put, a flow in IFM can trigger another flow. For example, receiving an order from a buyer triggers creation of an invoice by the seller, as shown in Figure 5 (dashed arrow).

To simplify the discussion, in the "panopticon" example, we assume an informational panopticon where monitoring involves all informational activities: receiving, processing, creation, releasing, and transferring, in addition to all secondary activities such as copying, destroying, and storing in each of the five stages of IFM. Any of these activities triggers receipt of information by the monitoring person, as shown in Figure 6. Thus, ethical evaluations can be made of different situations, for example, monitoring only transferred information (e.g., e-mail), or monitoring created information (e.g., updating and modifying operations in database systems).
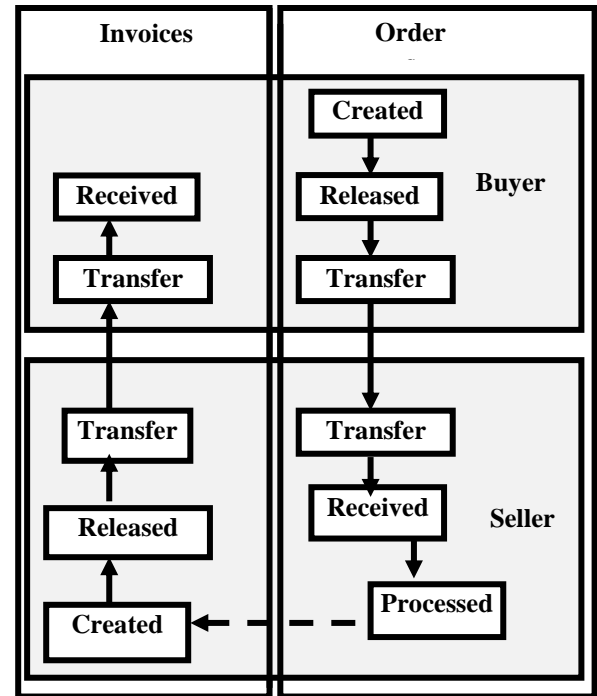

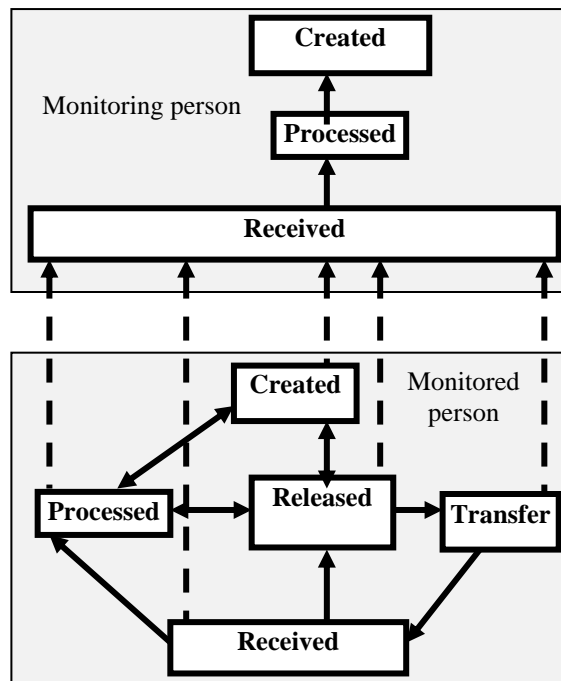Figure 5. Order flow triggers invoice flow.

Figure 6. Description of information panopticon.

VII. FUNDAMENTAL PRINCIPLES OF IE

The notion of entropy is a well-known concept that refers to destruction or corruption of information. Floridi's IE holds that information has an intrinsic worthiness, and "IE evaluates the duty of any moral agent in terms of contribution to the growth of the infosphere" (the information environment). Hence, according to [6], the fundamental principles of IE are the following:

0. Entropy ought not to be caused in the infosphere (null law);
1. Entropy ought to be prevented in the infosphere;
2. Entropy ought to be removed from the infosphere;
3. The flourishing of informational entities as well as of the whole infosphere ought to be promoted by preserving, cultivating and enriching their properties.

In IFM, entropy arises anywhere in the stream of information flow, while information increases from two sources: internal *creation* of new information, and *receipt* of information from outside the local information sphere. In thermodynamic entropy, the distribution of heat increases entropy; however, distribution of information does not increase entropy because transferring information to other infospheres (sending a copy) does not decrease information at the source.

The systematic description of the life cycle of information in IFM provides a fascinating opportunity to explore issues related to information and entropy.

REFERENCES

[1] S, Al-Fedaghi, "The ethics of information: What is valued most," Open Ethics J., vol. 3, 2009.

[2] S. Al-Fedaghi and B. Thalheim, "Personal information databases," Int. J. Comput. Sci. Inform. Secur. vol. 5, no. 1, pp. 11-20, 2009, USA.

[3] S. Al-Fedaghi, "Drafting informational privacy laws: Computer science perspective," Issues Inform. Syst., vol. 9, 2009.

[4] S. Al-Fedaghi, "Modeling aspects of action theory", Eighth International Conference of Computer Ethics: Philosophical Enquiry (CEPE 2009), 26-28 June 2009, Ionian Academy, Corfu, Greece.

[5] T. Bynum, "Computer ethics: Basic concepts and historical overview," in The Stanford Encyclopedia of Philosophy, E. N. Zalta, Ed. http://plato.stanford.edu/archives/win2001/entries/ethics-computer/.

[6] I. Floridi, "Information ethics, its nature and scope," in Moral Philosophy and Information Technology, J. van den Hoven and J. Weckert, Eds. Cambridge: Cambridge University Press, 2006.

[7] I. Floridi, "Information ethics: On the theoretical foundations of computer ethics", Ethics Inform. Technol. vol. 1, no. 1, pp. 37-56, 1999a. Reprinted, with some modifications, in The Ethicomp Journal, vol. 1 no. 1, 2004, http://www.ccsr.cse.dmu.ac.uk/journal/articles/floridi_l_philosophical.pdf

[8] I. Floridi, Philosophy and Computing: An Introduction. London: Routledge, 1999b.

[9] I. Floridi, "Information ethics: On the philosophical foundation of computer ethics." Proc. 4th International Conference on Ethical Issues of Information Technology (ETHICOMP98), Rotterdam, The Netherlands, 1998.

[10] I. Floridi, "Information ethics: An environmental approach to the digital divide," Philosophy in the Contemporary World, vol. 9, no. 1, pp. 39-45. UNESCO World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), Sub-Commission on the Ethics of the Information Society (UNESCO, Paris, June 18-19, 2001).

[11] I. Floridi, "Information" in The Blackwell Guide to the Philosophy of Computing and Information, L. Floridi, Ed. Oxford: Blackwell, 2006, pp. 40-61.

[12] T. J. Froehlich, "A brief history of information ethics," Bid, textos universitaris de biblioteconomia i documentació, número 13, desembre 2004, Accessed Oct. 2009. http://www.ub.es/bid/13froel2.htm

[13] K. Mather, "Object oriented goodness: A response to Mathiesen's 'What Is Information Ethics?'" Computers and Society, vol. 34, no. 4, 2005, http://www.computersandsociety.org/sigcas_ofthefuture2/sigcas/subpage/sub_pa ge.cfm?article=919&page_number_nb=911

[14] K. Mathiesen, "What is information ethics?" Computers and Society, vol. 32, no. 8, 2004, http://www.computersandsociety.org/sigcas_ofthefuture2/sigcas/subpage/sub_pa ge.cfm?article=909&page_number_nb=901.

[15] J. Rawls, A Theory of Justice, rev. ed. Oxford: Oxford University Press, 1999.

[16] M. M. Smith, "Information ethics: An hermeneutical analysis of an emerging area in applied ethics," Ph.D. thesis, The University of North Carolina at Chapel Hill, 1996.