20 REPRESENTING HUMAN AND NON-HUMAN STAKEHOLDERS: ON SPEAKING WITH AUTHORITY

Athanasia Pouloudi
Brunel University
United Kingdom

Edgar A. Whitley
London School of Economics and Political Science
United Kingdom

Abstract

Information systems research is concerned with complex imbroglios of human and non-human components. As researchers, we need ways to represent the intricacies of the different stakeholders in such situations. Traditionally, it is assumed that representing the views of human stakeholders is relatively unproblematic, but that doing this for non-humans is far more complex. This paper addresses this assumption, drawing on the philosophy of science of Isabelle Stengers. It considers the case of the UK NHSnet project and focuses on two stakeholders in the project, one human (the patients) and one non-human (the encryption algorithm used to encode confidential patient data). As the case study shows, representing either stakeholder is equally problematic and the paper reflects on the implications of this for information systems research.

1. Introduction

In the past five years, a new theoretical approach has been included in the range of perspectives used to study the phenomena of information systems. This approach is

typically known as actor-network theory (although there many problems with this name [Latour 1997, 1998] and the very act of naming [Law 1998]). Its origins can be found in the social studies of science (Bijker, Hughes, and Pinch 1987) and technology (MacKenzie and Wajcman 1999b), and in constructivist perspectives on the world (Callon 1998).

It is not easy to try to identify the core of what is meant by actor-network theory, or the sociology of translation, "[F]or the act of naming suggests that its center has been fixed, pinned down, rendered definite. That it has been turned into a specific strategy with an obligatory point of passage, a definite intellectual place within an equally definite intellectual space" (Law 1998 p. 2). Trying to fix on a single identity of the theory poses a danger to "productive thinking." It is possible, however, to identify certain characteristics found in most applications of these ideas. Of most importance to the information systems field is the emphasis that the approach puts on non-human actors, whether they be "natural" objects or man-made artifacts, although the distinction between humans and non-humans is much older. In the context of information systems, these are things we label as computers, networks, and organizations (Bloomfield and Vurdubakis 1994).

Actor-network theories suggest that non-humans are an essential component of any human activity system (if they are not, then society must be conceived as if it were constructed by human beings using their voices and naked bodies alone [MacKenzie and Wajcman 1999a, p. 24]). At one level, this is (with hindsight) an obvious contribution and one that can be accepted without much contention. Disagreements arise, however, when considering how this basic notion ("remember to include the non-humans") is operationalized.

One common technique is for the users of the theories to undertake a "semiotic turn" whereby all non-humans become semiotic devices that create texts alongside the texts created by the humans and these texts are analyzed with no consideration given to the nature of their producer. In so doing, however, they are open to criticism that they are ignoring the moral consequences of action (Walsham 1997, p. 473). Against this argument, Grint and Woolgar argue that actor-network theories are to be preferred to perspectives that implicitly or explicitly incorporate a technicist essence to technology and are thus guilty of technological determinism (Grint and Woolgar 1997).

A different kind of argument is presented by Collins and Yearley (1992a, 1992b) who point out that this approach takes Bloor's (Barnes, Bloor, and Henry 1996) principle of symmetry, whereby truth and falsity should be seen the same way, to many more dimensions. In so doing, it removes the human from the pivotal role of having special access to an independent realm (Collins and Yearley 1992a, p. 310). Given the overwhelmingly technicist view of much systems development discourse, it is perhaps unsurprising that many information systems researchers share the concern about displacing human agency from the center of information systems research.

Even if researchers are prepared to accept the moral questions associated with actor-network theories, a further concern is often raised by those considering using this approach (Latour 1999, p. 303): How are non-humans to be represented? How are they to be articulated? How do non-human actors speak? How can I be assured that I reliably report what they are saying? Implicit in such questions highlighting the problems of representing non-humans is the belief that applying these issues to humans is non-

problematic. Thus, it is presumed to be unproblematic to have human actors speak and to report what they are saying reliably.

This paper will argue that this distinction is not as clear cut as one would expect. It will do this by first considering, from a methodological point of view, what is involved in representing or speaking on behalf of actors (both non-human and human). It will then present an empirical example that has been reviewed with the added sensitivity to questions of speaking authoritatively on behalf of humans and non-humans. As the example will show, the question of how different kinds of actors are presented is not straightforward. Finally, the paper will draw implications for information systems researchers.

2. Speaking with Authority

When researchers enter a research situation, one of their objectives is to be able to say something about the situation under investigation. The researchers hope to speak authoritatively about this situation, to represent what is going on there. They may do this by describing in detail the features of the one situation, they may also wish to draw on the results from this one instance to say things about a general class of situations, of which the research site is but one typical (or atypical) location. This section will explore the theoretical conditions that underlie the claim that the researchers are speaking authoritatively about the situation and, following from the previous section, it will consider this question in relation to speaking authoritatively about the human and non-human elements of the situation.

2.1 An Issue Based Focus

The first point to be explicitly stated relates to the fact that, even if we are dealing only with human actors, the subjects of the study can have many things to say about a whole host of issues completely unrelated to the research question under investigation. In practice, researchers are always filtering information in this way, excluding issues that are unrelated and focusing on those that address the question. Obviously, this filtering carries the risk that some of the excluded information will, in fact, be vital for a proper understanding of the situation (Whitley 1999), but it happens nevertheless. Moreover, the stakeholders involved will change over time (Pouloudi and Whitley 1996).

In operationalizing this filtering process, the researchers may choose to conduct semi-structured interviews based on a topic guide (Pouloudi and Whitley 1996) with the goal of obtaining a better understanding of a particular situation or process. When studying non-humans, a similar filtering needs to take place. The new computer system can have implications on the air-conditioning in the building, on the security procedures enacted by the organization, and on the relative efficiency of the business. Researchers, however, may only be interested in how the particular computer system transforms the culture of different subgroups, for example, by providing fora for allowing individuals to discuss issues of common interest (Hayes and Walsham 1999).

2.2 "Let the Facts Speak for Themselves"

The second issue to be addressed relates to the fact that non-humans (especially technologically based non-humans) do not normally have the power of independent speech. Humans can vocalize what they want to say about a particular issue. How can a non-human do the same? Without the power of speech, how can the "interests" of non-humans be represented? Ironically, the answer to this can be found in the many opponents of constructivist accounts of science and technology. Instead of focusing on the social processes that lead to the development and stabilization of new scientific facts (Collins and Pinch 1993), the critics argue that nature provides the answer to these questions: "let the facts speak for themselves" is a common refrain.

Thus, in one sense, we already have experts who can allow the non-humans we are studying to speak, we simply need to ensure that they ask them the right questions about the topic under investigation.

In the case of humans, the process of articulation appears to be much more straightforward. We simply ask them about the particular topic and record their responses. Of course, depending on our theoretical preferences, we can make this process more sophisticated, for example, by undertaking a detailed analysis of the terms used, by exploring the hidden agendas lying behind the spoken utterances. In situations where we are potentially dealing with many humans, we may have to rely on questioning a subset of the group we are interested in, but assuming our statistical sampling is rigorous, this should not be a problem.

2.3 Authors and Authority

One further clarification needs to be made at this point and from this we will be able to generalize what we mean by speaking authoritatively. To help with this, the paper draws on the work of Isabelle Stengers, who argues that there is ambiguity about what we mean by being the author of a scientific fact. Thus the researcher can either be "an author, as an individual animated by intentions, projects, and ambitions" or the researcher can be "the author acting as authority" (Stengers 1997, p. 160). As Stengers points out,

> every scientist knows that he and his colleagues are "authors" in the first sense of the term and that this does not matter. What does matter is that his colleagues be constrained to recognize that they cannot turn this title of author into an argument against him, that they cannot localize the flaw that would allow them to affirm that the one who claims "to have made nature speak" has in fact spoken in its place. [Stengers 1997, p. 160]

What the scientist needs in order to speak authoritatively is the second form of authorship, the second form of authority. Given that the world can generally be interpreted in a number of different ways, what is required is "the active invention of ways of constituting the world that is under interrogation, as a reliable witness, as a guarantor for the one who speaks in its name" (Stengers 1997, p. 161).

Moreover, the statement being made must also be interesting. Where "to interest someone in something does not necessarily mean to gratify someone's desire for power, money, or fame" (Stengers 1997, p. 83). Being interesting also does not mean simply entering it into a network of preexisting interests. Rather, for Stengers,

> To interest someone in something means, first and above all, to act in such a way that this thing—apparatus, argument, or hypothesis in the case of scientists—can concern the person, intervene in his or her life, and eventually transform it. An interested person will ask the question: can I incorporate this "thing" into my research? Can I refer to the results of this type of measurement? Do I have to take account of them? Can I accept this argument and its possible consequences for my object? In other words, can I be situated by this proposition, can it place itself between my work and that of the one who proposes it? This is a serious question. The acceptance of a proposition is a risk that can, if the case arises, ruin years of work. [1997, pp. 83-84]

Thus, in this view, researchers must be seeking to have the phenomena they are studying speaking actively about interesting questions. Here Stengers has been referring to non-human actors. The situation becomes increasingly complicated when the phenomena under study are humans (or rats and baboons) who "are capable of interesting themselves in the questions that are asked of them" (Stengers 1997, p. 172) because they are able to interpret the sense of the apparatus that is interrogating them into their responses. In these cases, the notion of a witness becomes very problematic.

> The scientist is dealing with beings who are capable of obeying him, or attempting to satisfy him, or agreeing, in the name of science, to reply to questions that are without interest as if they were relevant, indeed, even allowing themselves to be persuaded that they are interesting, since the scientist "knows best." [1997, p. 172]

One obvious example of these problems can be found in Stanley Milgram's infamous study that created the conditions under which normal individuals became torturers. For Stengers, this study did not produce reliable witnesses because it

> reproduced, in an experimental setting, the perplexity that human history constrains us to. Milgram's torturer-subjects knew they were at the service of science, and this knowledge had as a consequence that the experiment, which was supposed to restrict itself to bringing a behavior to light, without doubt contributed, in an uncontrollable way, to producing this behavior. If a living being is capable of learning, which is also to say of defining itself in relation to a situation, the protocol that aims to constitute this living being as a reliable witness in the experimental mode and thereby constrain it to reply in a univocal way to a question decided by the experimenter creates an artifact. [1997, pp. 172-173]

This principle can be restated in a different way. Questions of authorship, or the authority of a text, cannot be resolved by relying on situations in which the researchers "master all the inputs and outputs and leave the objects no other freedom than the ability to say 'yea' or 'nay'!" (Latour 1997, p. xvi).

This section has introduced a series of issues associated with representing and speaking on behalf of humans and non-humans. The complexity of these issues will be considered in the context of a national network for health service employees, introduced in the next section.

3. The NHSnet

The NHS Executive, the body responsible for the execution of health care policy in Britain (NHS Executive 1994b), launched the NHS-wide networking project in 1993, as "an integrated approach to interorganizational communications within the NHS" (NHS Executive 1994a, p. 6). The objective of this network has been to enhance communication and information exchange between various health care providers and administrators. Thus, the NHSnet is expected to support data communications that cover a variety of information flows across different levels. Its infrastructure is expected to cover a variety of business areas, including patient related service delivery, patient related administration, commissioning and contracting, information services, management related flows and supplies of NHS organizations (NHS Executive 1995).

The NHSnet has been available since 1996. Yet, despite the technological success of the project, and in particular its completion within schedule, its implementation has suffered from a lack of acceptance by the medical profession. Doctors remain skeptical mainly of the security that the network has to offer. These concerns have been overtly voiced, mainly by the British Medical Association (BMA), the national professional body of physicians in the United Kingdom, but also by computer security consultants. These parties fear that patient data may be misused by both NHS members (referred to as "insiders") and external parties (Willcox 1995). As a result of their concern, doctors, again through the BMA, threatened not to participate in the electronic exchange of data unless they could be convinced that patient privacy is safeguarded.

In response to the criticisms, the NHS Executive has stated that the proposed system will be better than the previous situation: data confidentiality was quoted as one of the shortcomings of the previous situation and one that the NHS-wide networking infrastructure would safeguard (NHS Executive 1994a). Recently, the network has been described as "the best medium for the transfer of clinical information" (NHS Executive 1998b). However, the concerns on confidentiality and patient-identifiable information and the debates about alternative solutions have been ongoing since the network became available (e.g., Barber 1998b; Turner 1998) and remain unresolved. Indicative is the slow uptake of the network by GPs: fewer than 10% of GPs were fully linked to the NHSnet in April 1999 (Clark 1999). Still, the Health Secretary stated that all computerized GP surgeries are expected to connect to the NHSnet by the end of the 1999 financial year.

The next sections consider two important stakeholders in the problematic history of the NHSnet. We look at patients, a human stakeholder, and at encryption algorithms, a

non-human stakeholder. Both are key stakeholders in the debate about the security of the network and safeguarding the confidentiality of patient data. Importantly, they both raise some interesting and important issues about authorship and "speaking for" that are exemplified in the following discussion.

4. Patients

When it comes to healthcare provision, the most obvious stakeholder is the beneficiary, the patient. This section considers this process in the NHSnet case and provides an insight in the different approaches used by stakeholders to claim the right to speak for patients. Interestingly, the patient is also the party least involved in any discussions about how healthcare will be delivered and what processes will support this delivery. The interests of the patients, therefore, need to be represented by other stakeholders who claim to "speak with authority" on their behalf. Moreover, it is the argument that these stakeholders speak in the interests of patients that is used to give legitimacy to their views. It is interesting to note how this is reflected not only in the arguments of NHS members but also at a political level:

> But I know that one of the main reasons people elected a new Government on May 1st was their concern that the NHS was failing them and their families. [Foreword by the Prime Minister in *The New NHS,* Department of Health, 1997]

At the NHS Executive level, the representation of the interests of the patients is in recommending the use of the network: "Effective communications are vital to good patient care" (NHS Executive 1998a). The doctors' response, as we have discussed previously, was to react to the use of the network by arguing that it does not provide adequate safeguards for confidential patient data. Interestingly, not all GPs were aware of (and, therefore, concerned about) these shortcomings of the network. It has only been since the BMA raised the issue of confidentiality that doctors realized the risks for patients' privacy. The medical profession has since consistently argued that personal medical data can only be exchanged across a network that is safe from interception and received only by the professionals who need this information to provide care. The Data Protection Registrar also represents the interests of the patients, particularly since the enhanced provisions of the Data Protection Act of 1998 will shortly come into effect. In the case of the NHSnet, the Registrar has supported the BMA's concerns without becoming explicitly involved in the conflict over the network's use.

It should be noted that such smooth "nested" representation (the BMA representing the doctors or the Data Protection Registrar who represent the patients' interests) may be difficult to sustain as other interests of stakeholders are manifested. In the case of the NHSnet, the representation was effective because of the uniform reaction of doctors to the confidentiality issue:

> Each local medical committee decides whether it supports the BMA's position and so far each committee has universally supported the

> BMA's position on [the NHSnet] to the point that there was no dissent and that's because confidentiality is so closely linked to the general practitioners' hearts really. [Secretary to a group of local medical committees]

Some stakeholders question, however, the sincerity of the doctors' concerns about the patients. For example, employees of the NHS Executive have argued that the doctors, by adhering to the principles of data confidentiality, are in fact trying to keep close control over their patient information, which they have personally collected and which, therefore, defines—to an extent—their professional role. Other stakeholders, including some patients groups, argue that doctors resent sharing of patient information because the patient disclosed the information to a particular trusted GP. Making this information more widely available would damage the confidence of the patient and the consequently the doctor-patient relationship. The doctors fear that patients may then refuse to disclose sensitive information to the doctor, with unpredictable effects for diagnosis and hence the provision of appropriate care.

For this reason, the consent of the patient for the use of their private medical data has gained primary importance. However, since specific guidelines on consent arrangements are not available, doctors often rely on a notion of *implied consent* by the patient allowing doctors to share such data with other health professionals when appropriate. In other words, it is assumed that the patients rely on the professional *judgement* of their doctor in a given *context*. However, if this data is exchanged through an electronic network, and particularly if patient information is held centrally where healthcare professionals can access it, the notion of patient consent becomes extremely problematic. More importantly, the healthcare professionals (and support staff) accessing the information may be unable to view this information in relation to the context in which the patient disclosed the information. Thus, the relevance, or not, of some information may be difficult to judge (Introna and Pouloudi 1999). This is an indication that a non-human stakeholder, the network, can alter the representation context and its implications. This is more evident in this case study in the use of encryption, as illustrated in the next section.

5. Encryption Algorithm

Following the complex NHSnet debate on the confidentiality of personal medical data and the appropriate representation of patients, it is not surprising that the NHS Executive attempted to promote some formal mechanisms to safeguard access to such data. Thus, in response to the doctors' anxiety about confidentiality, and in order to avoid the cost of another spectacular system failure in the NHS (cf., Beynon-Davies 1995), the NHS Executive (and the government) have responded with a reconsideration of the security issue of the network. The Information Management Group of the NHS Executive commissioned Zergo Limited to "undertake a study looking at the ramifications of using encryption and related services across the NHS-Wide Network" (NHS Executive 1996). The Zergo report proposed the use of encryption to safeguard the privacy of medical records and was considered as "the solution" to the confidentiality problem by the NHS Executive:

> The measures we have put in place are to stop anybody who is unauthorized getting at data from and via, the [NHS-wide networking] system and one of the key parts of that system is a strong authentication challenge. [Statement by Ray Rogers, then Executive Director, NHS Information Management Group in Healthcare Computing 1996]

More specifically, the Zergo report put forward the use of the Red Pike encryption algorithm. This was devised by the *Communications-Electronics Security Group (CESG),* the information security arm of the *Government Communications Headquarters (GCHQ)* and the government's national technical authority on information technology and communications security. Thus, it would enable GCHQ to have access to the data transmitted over the NHSnet.

> The use of encryption for large and diverse applications such as the NHSnet is a new field and until recently none of the available encryption systems was sufficiently robust and comprehensive to suit NHS purposes. Implementation of Red Pike poses significant challenges but looks practicable. [NHS Executive 1996]

The suggestion raised new concerns within the BMA. Computer security consultants became actively involved. Ross Anderson, who has been consulting with the BMA on security matters, has been the one voicing most of the Association's concerns on their behalf and participating in the conflict with the NHS and the Department of Health:

> The Red Pike encryption algorithm is politically unacceptable, technically way out of date and won't command public confidence. [Ross Anderson, quoted in the *British Journal of Healthcare Computing and Information Management* (13:4), 1996, p. 6]

The NHS Executive has used encryption to speak for the issue of security and ultimately of confidentiality of patient data. Their suppliers have supported this view: "Firewall-to-firewall encryption could potentially act as an enhancement to NHSnet security and go some way to placating the BMA" (McCafferty 1996). In order to face the challenge, the BMA have formed alliances with privacy activists (e.g., Privacy International) and academics, on one hand, in order to raise the profile of the debate. On the other hand, they have created an alliance with security consultants, in order to challenge the technical features of the network as well. Thus, the BMA debated which encryption algorithm would satisfy the NHS needs best. Security and privacy specialists have also become involved in the debate to create awareness in the patient population about the dangers of the electronic exchange of healthcare data (Anderson 1996; Bywater and Wilkins 1996; Davies 1996). In this process, the encryption algorithm became a central non-human stakeholder, to whom the different human stakeholders attributed a number of (diverse, even conflicting) attributes, implying the inscription of diverse human stakeholders' interests, as the following quotations illustrate:

> In making information secure from unwanted eavesdropping, interception, and theft, strong encryption has an ancillary effect; it becomes more difficult for law enforcement to conduct certain kinds of surreptitious electronic surveillance (particularly wiretapping) against suspected criminals without the knowledge and assistance of the target. This difficulty is at the core of the debate over key recovery. [Abelson et al. 1998]

> Key recovery systems are particularly vulnerable to compromise by authorized individuals who abuse or misuse their positions. [Abelson et al. 1998].

> In the case of Trusted Third Party (TTP), you do have to trust the central authority and if some of the data warehousing organizations with links to insurance companies etc. manage to get the key they will have access to all patient records. It's not clear from the Zergo report why TTP was chosen over RSA....If we do go TTP, what will be the legal liability, if there is a security lapse? [Representative of Scientists for Labour]

> The level of confidentiality changes according to the social situation of the patient. [Kaihara 1998, p. 6]

> [T]he security of the stored data is not just a matter of technology but also of administrative procedures. [Kaihara 1998, p. 7]

> Ironically, total data encryption systems such as Pretty Good Privacy (PGP) are not compromised. But the NHS Executive has rejected systems such as PGP for the overall network. According to Ross Anderson, this is due to pressure from GCHQ which wants to control tightly the use of data encryption. The NHS Executive claims that systems such as PGP are unnecessary and cites cost and performance issues. [*British Journal of Healthcare Computing and Information Management* (13:3), 1996, p. 8]

> From the point of view of security standards within the NHS the key issue is that, whereas confidentiality has always been seen as a key issue in the handling of patient information, it is sometimes not addressed as seriously as it should be. [Barber and Skerman 1996, p. 35. Note that both authors are security consultants to the NHS Executive.]

> Although the concept of the confidentiality of personal medical data is well accepted by the general public and by health professionals, the detailed practice is under potentially serious attack by governments that want access in order to combat fraud or serious crime or to

> improve efficiency of services, by big business that wishes to improve its competitive edge or reduce its costs by utilizing detailed personal data in order to focus the promotion of its product and services and by health care organizations that do not keep their security measures up to the "state of the art" required by the information processing facilities available and the attacks on its personal medical data. All security measures need to be under constant review. [Barber 1998a, p. 25]

Despite the debatable role of encryption, the Zergo report was interpreted as a willingness of the government to take the doctors' concerns over security and confidentiality seriously. Thus, it signaled some progress in the resolution of the NHSnet debate at the time. Following the debate, the NHS Executive has now made explicit its view of the NHSnet as a "secure national network" (NHS Executive 1998a), effectively redefining the network. However, it did not manage to persuade doctors that the proposed system was secure, even though it was considered to be better than its predecessors, *ad hoc* manual and electronic exchange systems. The use of the NHSnet is still hindered by technical, organizational and cultural issues (*Computer Weekly News* 1999a, 199b, 199c).

The dialogues and conflicts between the NHSnet stakeholders indicate that some assume that encryption implementation warrants security. However, this assumption is problematic because it is a technical solution to a problem that is at the same time technical, organizational, political, and social. Furthermore, this assumption has repercussions for access to confidential patient data. In particular, if formal rules for such access are established at a national level, it is likely that professional discretion about disclosing personal medical data to appropriate recipients on a "need-to-know" basis will no longer be required. This impact has already caused the professional reaction of the medical profession as the role of the human stakeholder is diluted. More importantly, there is a danger that personal medical data become widely accessible to doctors at a national level, so that they can be accessed when necessary. While this is expected to have important benefits for the delivery of health care, it will be less evident to determine in which cases such data could be accessed and by whom. Any attempt to set specific rules would "remove the context" of professional judgement (and that could have severe implications, cf. Introna and Pouloudi 1999). Conversely, absence of rules would leave the system open to interpretation and possibly abuse of access rights, particularly if those accessing the information are not subject to rigorous professional obligations (Barber 1998b).

It is noteworthy that in arguing for or against the use of this non-human stakeholder, the issue of representation and speaking for the human stakeholder discussed previously, the patient, becomes relevant once more. Some security consultants describe the conflict on network security and encryption as a conflict, in essence, between the interests of the government and the end users (Abelson et al. 1998)—in this case the patients. The NHSnet security debate was manifested as a discord between the NHS Executive and the British Medical Association, representing the government and the patients respectively.

In information system research, it has been argued that non-human stakeholders, such as information and communication technologies, are not neutral, not least because they inscribe human values (Walsham 1997). In the case of the NHSnet, we can also observe how such inscribed values are interpreted in different ways by the stakeholders. In this

section, we demonstrated how different stakeholders attributed different values and interests to the non-human stakeholder, that is the security mechanism, in particular the encryption algorithm, to be used on the network.

6. Summary and Discussion

This paper has illustrated the different ways in which humans and non-humans are represented through the examples of two stakeholders in the UK NHSnet project. One stakeholder was human (namely the patients), the other was non-human (the encryption algorithm used to secure patient data being transferred over the network). Table 1 lists the various candidates who claimed to represent the two stakeholders discussed in the paper, indicating how they articulated the concerns of the stakeholder and including a sample of what they articulated on the behalf of the stakeholder.

As the table makes clear, there are multiple authors seeking to represent the stakeholders. Each uses different forms to speak on behalf of the stakeholders and each says very different things about the stakeholder being represented. For example, in the case of the patients, the doctors, their professional body, and the Data Protection Registrar were all seeking to represent them authoritatively. The Data Protection Registrar has a legal requirement to speak on behalf of the patients, while the doctors, through their professional body, sought to take up the moral requirement to speak for them. Moreover, both the BMA and the Data Protection Registrar are viewed with some skepticism in some quarters. The BMA, in representing the interests of patients, could also be seen to be maintaining the privileged position of doctors in the health care network. Similarly, there is general concern about the role of any government agency in issues of personal privacy and this affects perceptions of the role of the Data Protection Registrar.

The situation for the non-human actor (the encryption algorithm) was also complicated. The different security consultants sought to legitimize their view of the technology by undermining those of the alternative representatives.

It is also interesting to note the situation in which this non-human was to be represented. The different consultants operated within a situation (which arose from the Zergo report) whereby the issue was one of *which* encryption algorithm to use that would balance the needs of the NHS and the rights of the patients, closing down the debate about whether encryption *per se* was an issue. Similarly, the formation of the Caldicott Committee obliged the BMA and its allied stakeholders to become less polemic to governmental proposals:

> The Caldicott Committee failed to lay down hard and fast rules for patient confidentiality but because it produced a list of "good intentions" it certainly made it harder for BMA and other concerned organizations like DIN to continue to breathe fire and brimstone about matters. In this the commission probably served its purpose well. [Chairman of the Doctor's Independent Network]

Table 1. Summary of the Different Perspective of the Possible Representatives of the Two Stakeholders Considered in the Paper

Stakeholder	Possible representatives	Means of articulation	Sample articulation
Patients			
	"Patients"	Not directly involved in debate	—
	Politicians	Public statements	Concerns that the NHS was failing them
	NHS Executive	Policy documents	Effective communication is vital for good care
	Doctors (BMA)	Lobbying. Refusal to use system	Inadequate safe-guards for confiden-tial patient data
	Data Protection Registrar	Rulings on data protection issues	Limited public statements
Encryption algorithm			
	"Algorithm"	Performance of system	—
	Information Management Group	Policy	Strong authenti-cation challenge
	Zergo Limited	Zergo Report	Propose Red pike encryption to protect patient data
	Ross Anderson (for the BMA)	Academic publications	Red pike is politi-cally unacceptable, technically out of date
	Suppliers	Academic publications	Firewall-to-firewall security will placate the BMA
	Privacy activists	Public statements	Algorithm is subject to abuse by autho-rized individuals who abuse their position

It is commonly assumed that it is straightforward to represent humans but that representing non-humans is problematic. As this paper, and the examples in it, have shown, this is clearly not the case; representing either is equally problematic. This raises important questions about how we choose to represent human and non-human actors in information systems research, how we allow them to articulate themselves, and how the results of those articulations are used. In raising this question, the purpose is methodological (although there are also clearly "moral" issues associated with how much agency we grant to non-humans). The paper, therefore, presents the first stage toward answering the question of what is the best way for information systems research to be conducted so that the various stakeholders in the situation, whether human or non-human, can be represented. Having demonstrated the problematic nature of representing both humans and non-humans further research is needed to apply and evaluate different ways of allowing them to be represented authoritatively.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., and Schneier, B. *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*, 1998 (http://www.cdt.org/crypto/risks98; accessed October 17, 1999).

Anderson, R. J. "Patient Confidentiality at Risk from NHS-wide Networking," in *Current Perspectives in Healthcare Computing Conference*, B Richards (ed.). Harrogate: BJHC Limited, 1996, pp. 687-692.

Barber, B. "Patient Data and Security: An Overview," *International Journal of Medical Informatics* (40), 1998a, pp. 19-30.

Barber, B. "Towards a Measure of Privacy," *British Journal of Healthcare Computing and Information Management* (15:1), 1998b, pp. 23-26.

Barber, B., and Skerman, P. "What Are Your Security Standards?" *British Journal of Healthcare Computing and Information Management* (13:6), 1996, pp. 34-35.

Barnes, B., Bloor, D., and Henry, J. *Scientific Knowledge: A Sociological Analysis*. London: Athlone, 1996.

Beynon-Davies, P. "Information Systems 'failure": The Case of the London Ambulance Service's Computer Aided Despatch Project," *European Journal of Information Systems* (4:3), 1995, pp. 171-184.

Bijker, W. E., Hughes, T. P., and Pinch, T. (eds.). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: The MIT Press, 1987.

Bloomfield, B. P., and Vurdubakis, T. "Boundary Disputes: Negotiating the Boundary between the Technical and the Social in the Development of IT Systems," *Information Technology & People* (7:1), 1994, pp. 9-24.

Bywater, M., and Wilkins, C. "Mystic Megabytes," *British Journal of Healthcare Computing and Information Management* (13:2), 1996, pp. 10-11.

Callon, M. (ed.). *The Laws of the Markets*. Oxford: Blackwell, 1998.

Clark, L. "NAO Report: A Surgical Strike on NHS IT Projects," *Computer Weekly News*, 6 May 1999.

Collins, H., and Yearley, S. "Epistemological Chicken," in *Science as Practice and Culture*, Andrew Pickering (ed.). Chicago: University of Chicago Press, 1992a, pp. 301-326.

Collins, H., and Yearley, S. "Journeys into Space," in *Science as Practice and Culture*, Andrew Pickering (ed.). Chicago: University of Chicago Press, 1992b, 369-389.

Collins, H. M., and Pinch, T. *The Golem: What Everyone Should Know About Science*. Cambridge: Cambridge University Press, 1993.

Computer Weekly News. "Executive Must Woo Doctors," 18 March 1999a.

Computer Weekly News. "Hospital Staff Boycott NHSnet Over Poor Performance," 15 April 1999b.

Computer Weekly News. "Opinion: NHSnet Scheme Suffered from Fatal Flaws," 18 March 1999c.

Davies, S. "Dystopia on the Health Superhighway," *The Information Society* (12), 1996, pp. 89-93.

Grint, K., and Woolgar, S. *The Machine at Work: Technology, Work and Organization*. Cambridge, England: Polity Press, 1997.

Hayes, N., and Walsham, G. "Safe Enclaves, Political Enclaves and Knowledge Working," paper delivered at the conference on Critical Management Studies, Manchester, 1999.

Introna, L., and Pouloudi, A. "Privacy in the Information Age: Stakeholders, Interests and Values," *Journal of Business Ethics* (22:1), 1999, pp. 27-38.

Kaihara, S. "Realization of the Computerized Medical Record: Relevance and Unsolved Problems," *International Journal of Medical Informatics* (49), 1998, pp. 1-8.

Latour, B. "On Actor-network Theory: A Few Clarifications," Centre for Social Theory and Technology, Keele University, United Kingdom, 1997.

Latour, B. "On Recalling ANT," in *Actor Network and After*, J. Law and J. Hassard (eds.). Oxford: Blackwell, 1998, pp. 15-25.

Latour, B. *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press, 1999.

Law, J. "After ANT: Complexity, Naming and Topology," in *Actor Network and After*, J. Law and J. (eds.). Oxford: Blackwell, 1998, 1-14.

MacKenzie, D., and Wajcman, J. "Introductory Essay and General Issues," in *The Social Shaping of Technology*, D. Mackenzie and J. Wajcman (eds.). Buckingham, England: Open University Press, 1999a, 3-27.

MacKenzie, D., and Wajcman, J. (eds.). *The Social Shaping of Technology*. Buckingham, England: Open University Press, 1999b.

McCafferty, C. "Securing the NHSnet," *British Journal of Healthcare Computing and Information Management* (13:8), 1996, pp. 24-26.

NHS Executive. *A Strategy for NHS-wide Networking*. No E5155, Information Management Group, 1994a.

NHS Executive. *This is the IMG: A Guide to the Information Management Group of the NHS Executive*. No. B2126, Information Management Group, 1994b.

NHS Executive. *NHS-wide Networking: Application Requirements Specification*. No. H8003, Information Management Group, 1995.

NHS Executive. *The Use of Encryption and Related Services with the the NHSnet: A Report for the NHS Executive by Zergo Limited*. No. E5254, Information Management Group, 1996.

NHS Executive. *IMG: Programmes and Project Summaries*. No. B2232, Information Management Group, 1998a.

NHS Executive. *Information for Health-Executive Summary*. No. A1104, Information Management Group, 1998b.

Pouloudi, A., and Whitley, E. A. "Stakeholder Analysis as a Longitudinal Approach to Interorganizational Systems Analysis," paper delivered at the Fourth European Conference on Information Systems, Lisbon, Portugal, 1996.

Stengers, I. *Power and Invention: Situating Science*. Minneapolis: University of Minnesota Press, 1997.

Turner, R. "The Caldicott Committee Reports," *British Journal of Healthcare Computing and Information Management* (15:1), 1998, pp. 23-26.

Walsham, G. "Actor-Network Theory and IS Research: Current Status and Future Prosjects," in *Information Systems and Qualitative Research*, A. S. Lee, J. Liebenau, and J. I. DeGross (eds.). London: Chapman & Hall, 1997, pp. 466-480.

Whitley, E. A. "Understanding Participation in Entrepreneurial Organizations: Some Hermeneutic Readings," *Journal of Information Technology* (14:2), 1999, pp. 193-202.

Willcox, D. "Health Scare," *Computing,* October 19, 1995, pp. 28-29.

About the Authors

Athanasia (Nancy) Pouloudi is a lecturer in the Department of Information Systems and Computing at Brunel University. She has a Ph.D. in "Stakeholder Analysis for Interorganizational Systems in Healthcare" from the London School of Economics and Political Science, an MSc in "Analysis, Design and Management of Information Systems" from the same university, and a First Degree in Informatics from the Athens University of Economics and Business. Her current research interests encompass organizational and social issues in information systems implementation, stakeholder analysis, electronic commerce and knowledge management. She has more than 20 papers in academic journals and international conferences in these areas. She is a member of the ACM, the Association for Information Systems (AIS), the UK AIS, and the UK OR Society. Nancy can be reached by e-mail at Nancy.Pouloudi@Brunel.ac.uk.

Edgar Whitley is a senior lecturer in Information Systems at the London School of Economics and Political Science. He has a BSc (Econ) Computing and a Ph.D. in Information Systems, both from the LSE. He has taught undergraduates, postgraduate students, and managers in the UK and abroad. Edgar was one of the organizers of the First European Conference on Information Systems and is actively involved in the coordination of future ECIS conferences. He has published widely on various information systems issues and is currently completing a book on the socio-philosophical foundations of information systems. Edgar can be reached by e-mail at E.A.Whitley@lse.ac.uk.