The integrity of creating, communicating and consuming information online in the context of Higher Education Institutions

Simon Rogerson[1]
Centre for Computing and Social Responsibility, Faculty of Technology, The Gateway, De Montfort University, U.K.

Introduction

Similar to all organizations, HEIs (Higher Education Institutions) are reliant on information to operate, report and provide services. There are unique relationships between the institution, the academic and the student. The success of the HEI depends on this relationship trinity and the existence of trusting relationships within it. The trinity is sustained through creating, communicating and consuming information that is increasingly electronic in form.

The integrity of an HEI is the bedrock on which an HEI's trustworthiness is founded. Such integrity is concerned with the quest for truth and knowledge by requiring intellectual and personal honesty in learning, teaching, research and service, and establishes standards and processes which promote fairness [1] in the interactions between the institution, the academic and the student. Information is an important element in realizing HEI integrity and thus establishing and sustaining a trustworthy HEI relationship trinity. Therefore the integrity of such information should be of the utmost concern.

The converging technologies to what is often referred to as ICT (information and communication technology) have changed the way we should look at information. ICT maturity has reached a point where information of nearly every form is available at the touch of a button, the click of a mouse or the pointing of a cursor. Never before has it been possible to support many-to-many or many-to-one information publication and consumption. Existing new information conduits such as tweets, blogs, podcasts and wikis offer so much. Access is now possible to all forms of information including music, moving images, literary works and art. Within HEIs the increasing use of technology-supported information of all kinds raises questions over information integrity and whether the information received can be trusted. Information integrity is about accuracy, consistency and reliability of information content and the hosting information systems. If information is questionable then decisions and actions that are based

[1]Email: srog@dmu.ac.uk

on it could be flawed and unsafe. The expectation that information has integrity and therefore is dependable and trustworthy is reasonable.

Without trustworthy information the HEI cannot function properly. The trustworthiness of the HEI itself is called into question. This paper explores these notions in detail and in doing so provides an agenda of issues that need to be addressed in order to increase the likelihood of trustworthy HEIs.

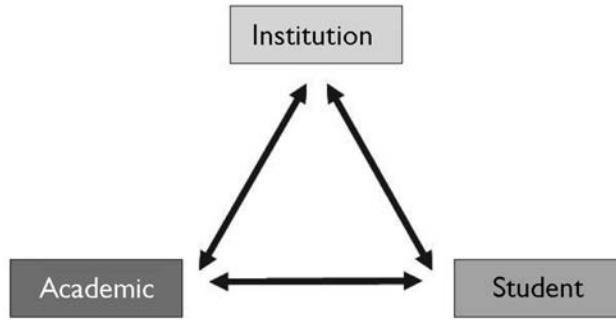
The HEI

In terms of its fundamental organizational focus of education provision in its broadest sense, any HEI comprises the institution, its academics and its students. The organization is represented by the administrators and managers. It is they who create and coordinate the institution. This would be those working in areas such as the executive, academic registry, finance, human resources, IT (information technology) and information services. The academics comprise those who have direct contact with students at different levels, be it pre-undergraduate, undergraduate, postgraduate or research. They might be permanently employed or employed on a fixed-term contract, they might be full-time or part-time members of staff. Students are any individuals who are enrolled with the HEI to undertake a programme of study. This could be for example, a foundation degree, undergraduate degree, a taught postgraduate degree, a research degree or a short course, which may or may not have an associated credit. Modes of study can vary along three perspectives: duration is full-time or part-time; engagement is face to face, distant or blended; and occurrence is on demand or scheduled.

Relationship trinity

Relationships exist between these entities of an HEI. This is defined as a relationship trinity as shown in Figure 1. If the trinity operates effectively then the HEI is well positioned to rise to the demanding challenge of delivering quality education provision, which is a particularly difficult challenge in the global economic climate of today. The relationship trinity will both be affected by and

Figure 1



The HEI relationship trinity

affect the educational culture, pedagogical strategy and the operational plan of the HEI. Relationships will be two-way between institution and academic, academic and student, and student and institution.

Trust across the relationship trinity and the resultant perceived trustworthiness of an HEI need to be explored. Smith [2] explains that trust is a social relationship where 'A' trusts 'B' to do 'C'. 'A' will only trust 'B' if 'A' believes 'B' to be trustworthy with respect to 'C' and for 'B' to be trustworthy requires that 'B' has both the competence and the motivation to satisfy the requirements of 'C'. Smith [2] further suggests that trust is relational in nature and this implies that trustworthiness is but one component of a larger social relationship of trust between actors. For example, in the delivery of e-learning within an HEI, a student will only trust an academic if the student believes that the academic is trustworthy with respect to e-learning and for the academic to be trustworthy requires that the academic has both the competence and the motivation to satisfy the requirements of e-learning. Therefore in the larger social relationship of trust, a student may distrust an academic regarding e-learning because either competence or motivation or both are lacking, but at the same time might trust the same academic regarding assessment of work because both competence and motivation are present.

Organizational trust is a specific type of trust between people and a social organization [2]. Trust in the organization is based on an expectation that the words, actions and promises of another individual or group can be relied on [3]. In terms of the relationship trinity, organizational trust means the trust between the HEI and both academics and students. Trust exists if academics and students have trust in the rules, roles and norms of the HEI regardless of the people who fulfil the roles defined here as administrators and managers. It is the organizational arrangements that ensure administrators and managers operate appropriately.

ICT and HEI trust

Trust takes on a new importance with the advent of ICT dependency. This is because there is widespread perception that the online world is problematic in terms of the integrity of information [4] related to all aspects of HEI activity. Secondly, the vital trusting relationship between student and academic is at risk without the cues of the real world [5]. Trusting relationships in the physical real world rely heavily on no verbal cues such as body language. In the virtual world such cues rarely exist. Thirdly, the increasing use of ICT can tilt the power balance in favour of those in control of the technology [2], which could have a detrimental effect on academic integrity.

There are many ICT-dependent areas within the relationship trinity, and typical areas will now be considered in turn. The areas discussed in total do not necessarily offer complete coverage, but they provide a sense of the pervasive nature of ICT in the HEI and therefore highlight the enormous potential impact ICT has on establishing a trustworthy HEI. It also highlights that it is the information that is created, communicated and consumed through ICT that is the crucial element rather than the technology itself.

Institution and academic

Accessing electronic journals, citation indices and reference databases is the traditional area of support for the academic and has seen an evolution from paper-based and non-book media in a traditional library setting to an electronic information resource that is on-demand and remote. Questions of legitimacy of electronic sources are widespread, and resources such as Wikipedia (http://www.wikipedia.org/) remain controversial regarding their use in academic work. Questions of trustworthiness of source material raise issues regarding the integrity of research and teaching. The institution provides academics with a variety of ICT tools to aid in course administration. It is now commonplace to assess students electronically, to submit marks electronically, and to create and submit examination papers electronically. In all cases the trustworthiness of these approaches relies on ICT being reliable and secure. Unreliable ICT means the information may or may not be available. Insecure ICT means information is compromised.

Academic and student

The trusting relationship between academic and student is fundamental to HEI provision. Damage this relationship and the HEI can be damaged beyond repair. ICT has had a great impact on this relationship. E-learning, either standalone or combined with classroom activity (known as blended learning), is common across both HEIs and disciplines. Students and academics interact online both professionally and socially through Web 2.0 facilities such as Skype (http://beta.skype.com/en/) and LinkedIn (http://www.linkedin.com/), which facilitate participatory information sharing. Students submit work through electronic coursework repositories to their academic tutors who in turn provide online summative and formative feedback. Academics can monitor student engagement in real time as well as retrospectively using ICT tracking and monitoring systems. This use of ICT challenges the manner in which trust is established between academic and student. In an online situation without any face-to-face cues, how can the identity of both student and academic be verified beyond reasonable doubt? If it cannot, then trust will be compromised. Tracking progress in the classroom can affect the relationship, for how can trust be sustained when the student knows he/she is under surveillance by the academic? Electronic access is possible to the work of others, be they peers or outsiders, offering an easy temptation to plagiarize. Software, such as Turnitin (http://turnitin.com/), is used to scrutinize submitted work. This policing process will inevitably damage the trusting relationship, because it implies the student has to demonstrate plagiarism has not taken place since there exists, in general, a suspicion that it has.

Student and institution

The relationship between student and institution has similarly changed with increased ICT usage. Student applications and records are now online, providing easy access and the ability to correlate information in different ways. There are much more flexible learning opportunities both on-campus and at a distance using a range of ICT tools for education. Students have a wide range of personal online resources including email, an electronic library, social networking and

campus-wide wireless connection. Identity cards with electronic capabilities, such as biometrics are now commonplace in HEIs and are used for building access and attendance monitoring. Access to ICT is expected by prospective students as they have grown up in a more technologically advanced age. The student's perception of the quality of such facilities will have an important impact on their perception of the trustworthiness of the organization. The manner in which identity cards are used by the HEI will impact on trust. Presented in a positive way for providing safe and exclusive access will benefit trust, whereas if it is presented as a means of surveillance and control, then trust will be damaged.

Types of communication

One aspect of this increasing use of ICT across the trinity is the increase in the types of communication that are now possible. Communication can be carried out on a one-to-one, one-to-many, many-to-one and many-to-many basis. For example, one-to-one communications occur when an academic enters into an email dialogue with a student about an assignment or when an academic submits marks to an institutional administrator. One-to-many communications occur, for example, when the institution broadcasts on the closed area of its website an announcement to the student population or when a student enters a learning resource area, is automatically recognized and the information is sent to relevant academics and institutional areas for authorization, monitoring, assessment and support purposes. Many-to-many communication can occur, for example, where a discussions board is created in a virtual learning environment so that students can debate freely issues relating to curriculum topics of a course. Many-to-one communications occur, for example, where the institution is seeking student feedback about course provision and the student experience or where an academic has set up an online automated test that each student of a course has to undertake at a specified time. Communication can be either one way or two way depending on particular facets of the relationship. For example, the one-to-one communication between academic and student described above is a two-way communication, whereas the institution's student feedback survey is a one-way communication. There can be situations where communication can vary. For example, an academic creates a blog relating to a course. The blog might start as a one-way, one-to-many communication. If a dialogue is triggered that involves students and the member of staff who would add new blog entries then the communication would become many-to-many and two-way. It is vital that all in the relationship trinity understand the nature of communication, for without that understanding communication can be distorted and inappropriate. That would adversely affect trust.

Information and the HEI

As explained earlier, it is information that sustains the relationships within the HEI. It is appropriate to consider information across the trinity in more general terms so that the link between information and HEI trust can be explored. Information can have its origins internally or externally to the trinity. Internal information is created by one or a combination of some of the three entities of

an HEI. It is then communicated to another entity or other entities where it is consumed. External information would take a similar path with the additional point of import. Of course, some information might be created by a combination of external agencies and internal HEI entities. The iCCC (information Create Communicate Consume) process [6] is an important concept in understanding the manner in which ICT-supported information is used to sustain relationships and whether such information can be trusted. If it cannot be trusted, then trust across the HEI is compromised.

The issue of trustworthy information pervades iCCC. The creator of a piece of information needs to consider who will be the recipient within the relationship trinity and in some cases beyond that trinity. The format must be fit for purpose for recipients, and the creator must ensure the information has integrity. The decision has to be taken as to the type of communication conduit to use. It is likely that the level of security will be a significant factor. The information must be meaningful for the consumer, who must be satisfied with the integrity of the information. Information will only be trustworthy if all these things are in place. For example, an academic emails a final year examination paper as an unencrypted attachment across the unsecure wireless network within the HEI to the institution's examination office. There is considerable doubt about the trustworthiness of this information. Email is a poor choice for communicating confidential information. The use of unencrypted attachments offers the opportunity for hacking. The hacking opportunity is made easier through the use of an insecure wireless network. Whether the examination paper is accessed by an unauthorized person or not is not the issue. The issue is that it might have been, so from the consumer's (the examination office) viewpoint the received information lacks integrity and therefore is untrustworthy. If this is common practice within the HEI then it is questionable whether the HEI can be trusted to undertake proper assessment of its students, and the awarded qualifications are themselves called into question.

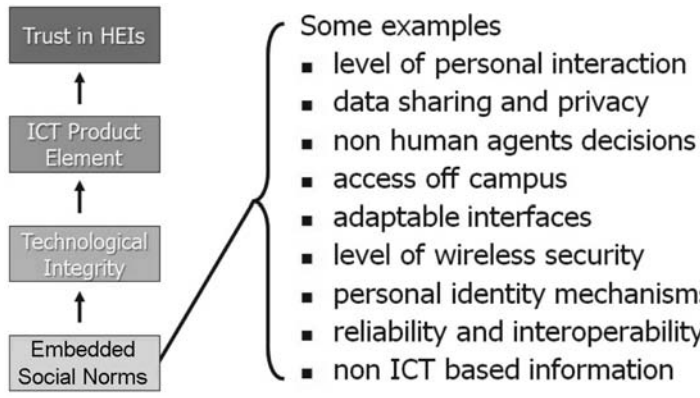
As mentioned earlier an increasing amount of information within an HEI is ICT-enabled and so the practice of ICT needs to be considered here. The development and operation of ICT practice has two distinct elements: process and product [6]. With regard to this discussion, the product element is of particular interest. The focus of the product element is technological integrity from, for example, a Kantian or utilitarian perspective. This can be addressed by embedding social norms within ICT products themselves. This might be as simple as building in 'opt-in' facilities in service provision via the Internet whereby a person must ask to be informed of future service offerings rather than having to request explicitly not to receive such information by default. For example, a student would have to opt in to get journal paper alerts on a particular topic via the HEI's electronic library. The embedding of social norms might be more complex than a simple tick box as was the case in the first example. It might involve a sophisticated, automated decision-making process. For example, a student has breached HEI regulations by sending out spam via the HEI email. This breach is fed to a non-human agent such as a student identity card system that is programmed with defined ethical principles so that it will only instigate actions that are deemed to be societally acceptable. Therefore it might restrict a student's access to certain facilities such as Internet access, but still allow the student to attend lectures.

It is the product element that is particularly relevant to the issue of ICT impact on trustworthiness in HEIs. Figure 2 shows how the embedded social norms lead to technological integrity of the ICT product. Using ICT products of this nature promotes trust within the relationship trinity and assists in establishing trustworthy HEIs.

The norms shown in Figure 2 are by way of illustration. Fit-for-purpose systems have embedded social norms. They provide the right level of personal interaction, interfaces that can be changed to suit an individual's specific needs, use in a secure way on and off campus across different networks, control of data sharing so valid privacy can be maintained, and interoperability, which enable access using a variety of hardware such a laptops, iPads and smart phones. These examples demonstrate the importance of careful consideration of including social norms in the design of ICT systems that will enable trustworthy iCCC throughout the relationship trinity of the HEI. ICT dependency will continue to increase, and consequently the impact on us all will be enormous. For the HEI, it is likely that most, if not all, information within the iCCC process will occur through ICT. The relationship trinity will therefore flourish or fail by the fortunes of ICT. The smallest failure in ICT will call into question its trustworthiness and consequently the trustworthiness of the HEI will be questioned. The ability to provide a measure of trustworthiness through, for example, a provenance model appears to be a reasonable way to tackle this issue.

Information integrity is about accuracy, consistency and reliability of information content [7]. If information is questionable then decisions and actions that are based on it could be flawed and unsafe. The expectation is that information has integrity and therefore is dependable and trustworthy. Consequently, decisions and actions have a firmer foundation and so are themselves more likely to be trustworthy. How can the trustworthiness of information be demonstrated? Trustworthiness is an intrinsic reality. Its perception, particularly in the beginning, depends critically on the perception of extrinsic forms such as signs, labels, messages etc. These are understood to represent the presence of underlying trustworthiness [8]. These extrinsic messages would provide the much-needed

Figure 2



Typical social norms in ICT products for HEIs

guide to information integrity. If such messages were recorded over time, then the information would exhibit a provenance. In general, provenance defines the place of origin and is a proof of authenticity or of past ownership. Therefore, information provenance fixes the origin and network of ownership, thus providing a measure of integrity, authenticity and trustworthiness. It provides an audit trail showing where information originated, where it has been and how it has been altered. This way, people throughout the relationship trinity would be able to consider how much credence they would give to a piece of information before acting on it. For any piece of information, people should be able to answer the following questions: Can this information be believed to be true? Who created it? Can its creator be trusted? What does it depend on? Can the information it depends on be believed to be true? [9]. The creators within the relationship trinity of information have a moral obligation to address information integrity, for it is information integrity on which HEI trustworthiness relies. Information provenance offers a normative instrument for turning this moral obligation into practice.

The information dichotomy

There is an interesting dichotomy in the technologically dependent Information Society. Information is the lifeblood of organizations in the information age [10], including HEIs. The veins of data communications along which this blood circulates are the new utility of the information society. Without communicated information an HEI cannot interact; the relationship trinity withers. With the advent of ICT as an ever-evolving technology, the amount and type of information available has exploded. Tofler [11] predicted this information overload, where individuals and organizations were swamped with so much information that it prevented decision-making and actually reduced knowledgex. This problem continues to grow at a seemingly accelerating rate. Indeed Nielsen [12] argues that we are reaching the point of saturation: "Information pollution is information overload taken to the extreme. It is where it stops being a burden and becomes an impediment to your ability to get your work done". Typical examples of information pollution in an HEI context are the overly complicated myriad of performance metrics for not only the institution, but also individual academics and students. ICT enables such metrics to be collected and so they are collected just in case they might be needed.

If humankind is going to survive this mutation of information lifeblood into information pollution, a new way of thinking and an associated new way of operating has to be derived. As Evans [13] remarked over 30 years ago, "Computers, in other words, have not arrived on the scene for aesthetic reasons, but because they are essential to the survival of a complex society, in a way that food, clothing, housing, education and health services are essential to a slightly simpler one. The truth is that one of the main problems – perhaps the main problem – of the time is that our world suffers from information overload, and we can no longer handle it unaided". One aid that could reverse this mutation is explicit guidance as to the status of information as it is presented. In other words, to provide a rating of the integrity of the information before it is consumed. This is information provenance.

It is true that we all need information all of the time. It is information that enables HEIs to exist and flourish. The converging technologies are transforming information and its access at an accelerating speed. The traditional information bearings have been demolished, which in turn threatens to send us into information meltdown. This meltdown can be avoided if we can curtail our insatiable appetite for information junk, replacing it with a controlled diet of quality information in an acceptable form and delivery on demand. Those in the relationship trinity need to learn how to benefit from this varied diet of fit-for-purpose information and how to judge whether information is trustworthy. That will help sustain trust in HEIs. If this is ignored, information meltdown will contribute to the eventual collapse of the HEI and herald a return to the Dark Ages rather than the dawn of a new Enlightenment.

Comments by Robert B. Kvavik[2]

Professor Rogerson's observations on the impact of IT and the cyber-infrastructure on trust among students, faculty and staff, and the administration (a triad of relationships in his terms) are noteworthy and inspire further elaboration.

Professor Rogerson's triad could be expanded to include other higher education clientele such as the general public, the government (state and local), research sponsors (public and private), donors, alumni and more. All parties are now connected to one another in a virtual administrative and learning community characterized by new patterns and modes of interaction, communication, visibility, expectations and outcomes.

Fundamental to any well-functioning community is trust. Basically trust implies a willingness by one individual or group to rely on another party's actions and an expectation that the other party's actions will be beneficial. Trust has unique characteristics when relationships are increasingly influenced by new and sometimes poorly understood IT systems.

During the last two decades, higher education has invested, by a conservative estimate, U.S. $10 billion in administrative and ERP (Enterprise Resource Planning) systems, learning systems and communication tools. These components tie together the universities' many learning communities. They afford new opportunities and ways to communicate, educate, administrate and generate support (chat groups, text messaging, e-mail and e-forums, personal links and list serves, wikis, social media, elections, surveys etc.).

For these relationships to work the systems that support them must be trusted systems, i.e. they do what is expected of them irrespective of human errors or environmental changes. And they must be trustworthy, i.e. they must be secure, available, reliable and protect privacy. In Professor Rogerson's terms, trust requires information integrity, which equals accuracy, consistency and reliability. By integrity he means dependability and trustworthiness. We would expand the definition of reliability when applied to ERP to include resilience and recoverability, to involve no disruption and to be production-ready and predictable. When IT systems fail

2 University of Minnesota, U.S.A. (Email: kvavik@umn.edu)

to perform to these standards, for whatever reason, trust among the parties can quickly erode.

Noteworthy are a number of areas that illustrate the new complexity of 'trusted relationships' and where behaviour and consequences can be difficult to manage and predict.

Identity management

Higher education enjoys a well-earned reputation for securing and integrating identity management within and among campuses. Determining and controlling who has legitimate access to IT provided services and when is basic to key university functions such as admission, registration, financial aid, on-line courses, grants management and purchasing. When students cannot register in timely fashion or accounting errors occur, trust quickly breaks down among the affected parties. What become scrutinized are the choice, implementation and maintenance of the systems, not to mention questions of fraud and malfeasance.

Social and administrative networks

As universities begin to adopt Google Docs, Facebook (http://www.facebook.com/) and Microsoft Office Live, the ability to manage, monitor and enforce privacy regulations, policies and expectations erode. Not only can this lead to lack of trust in dealings with the institution, it can incur severe fines for failure to conform to governmental regulations and ensuing liability suits. A related area is 'acceptable use' as it applies to copyright and diversion of campus resources to outside entities. Can vendors trust universities to adhere to the limitations of their service contracts? Enforcement can be problematic in a culture where traditionally access to information is free.

Blogs and chat groups make relationships among the key players in Rogerson's trinity increasingly bilateral or even trilateral rather than unilateral and unidirectional. Access to and consumption of information and opinions about universities, their faculty, reputation, finances and performances can radically change power relationships among the players. Better-informed students will be likely to make better choices and may or may not be influenced by university-controlled media, images and messaging. Bargaining among staff and the administration is improved when more information is on the table; at least, that is the hope. Universities by necessity must be more open and forthcoming in this new environment. Cover-up and obfuscation are hard to sustain in the information age, as a number of prominent politicians have learned recently.

Assessment

As more and more assessment of learning and faculty and staff performance goes online, policy and trust issues naturally arise concerning survey tools, their functionality and security, data collection and appraisal tools and methodology, and whether Fair Information Practice principles are followed.

Hacking, breach response and privacy

Ask any higher education CIO (Chief Information Officer) and they will tell you that hacking university systems is similar to a 'dragons and dungeons' game. Each

time you solve a problem, the next one gets harder, and you have fewer resources to solve it. The potential liability, both financial and to place trust in the system and institution, is enormous when personal information and research data are illegally or accidentally exposed. Nowhere is this more sensitive than with respect to patient data in university hospitals and medical facilities.

Protection of research data, data management and export control

Data no longer sit on paper in boxes in faculty and administrative offices. They rest in centralized repositories, whose managers are responsible for preservation, accessibility, confidentiality and security. The analysis of such data is often carried out on computers outside of the institutions, and in the most complex situations, Grid Technology is used. Identifying trusted users and securing data across transmission lines is increasingly complicated and costly.

Blended and online learning

The new IT technologies make possible blended and online learning, which changes how we teach, who we teach and when we teach. The accompanying new teaching paradigms and changing financial models, i.e. who pays, how and for what, are all evolving as are trusted relationships among the players in this domain.

This myriad of problems and opportunities constitute the new reality that Professor Rogerson so aptly describes. They also directly impact the three other themes of this conference: strengthening of the media, increasing call for accountability and rising stress on utility.

As universities become globally public, investment in media and communications increases in importance. It is probable that no administrative unit at the University of Minnesota has grown more rapidly in budget, media tools and strategies, and skilled personnel than institutional relations. What used to be limited to a few editors publishing glossy magazines, newsletters and Christmas calendars (that no one used), is now mostly online, using social media and elaborate networks, and tools such as customer relationship management. University presidents use Twitter (https://twitter.com/) and Facebook. Their every move is subject to IT-aided scrutiny, and in some instances, GPS tracking. In this exposed environment, trust is increasingly fragile and at the same time, more critical than ever.

As all university activity is increasingly visible to the public, demands for accountability invariably follow, ironically and conversely in relation to public funding. IT enables a more diverse and larger clientele to follow university performance, and this inevitably results in the need for equally diverse performance measures and reporting mechanisms.

Lastly, concomitant with public scrutiny of university priorities and educational objectives, and as the public pays directly more and more of the cost of running universities, it is not surprising that the value equation changes to one that is more utilitarian – applied research versus basic research; professional and occupational training versus liberal arts education; and mass education versus elite education.

In the U.S.A., trust for public institutions is at an all-time low. Although not as severe for government, corporations and religion, public support for universities and trust is lower than a decade ago. Do faculty teach enough? Are they

paid too much? Why are tuition fees increasing faster than the cost of living? Are institutions leaning politically to the left? Do political agendas colour research on the environment, sustainability, and drug and food safety? Have the universities sold out to the pharmaceutical companies and big business? In some societies, are they the agents of a repressive state? IT has made the ideal of the Ivory Tower totally irrelevant – at best fiction and at worst delusion.

References

1. The Center for Academic Integrity (1999) *The Fundamental Values of Academic Integrity*. The Center for Academic Integrity, Durham, NC
2. Smith, M.L. (2011) Limitations to building institutional trustworthiness through e-government: a comparative study of two e-services in Chile. *Journal of Information Technology* **26**, 78–93
3. Tschannen-Moran, M. and Hoy, W. (1998) Trust in schools: a conceptual and empirical analysis. *Journal of Educational Administration* **36**, 334–352
4. Kasprzak, J. and Nixon, M. (2004) Cheating in cyberspace: maintaining quality in online education. *Association for the Advancement of Computing In Education* **12**, 85–99
5. Hai-Jew, S. (2007) The trust factor in online instructor-led college courses. *Journal of Interactive Instruction Development* **19**, 11–25
6. Rogerson, S. (2010) A review of information ethics. *Journal of Information and Management* **30**, 6–18
7. Mandke, V.V. and Nayar, M.K. (2004) Beyond quality: the information integrity imperative. *Total Quality Management and Business Excellence* **15**, 645–654
8. McRobb, S. and Rogerson, S. (2004) Are they really listening? An investigation into published online privacy policies. *Information Technology and People* **17**, 442–461
9. Huang, J. and Fox, M.S. (2004) Uncertainty in knowledge provenance. In The Semantic Web: Research and Applications. Proceedings of the First European Semantic Web Symposium, Heraklion, Greece, 10–12 May 2004 (Bussler, C.J., Davies, J., Fensel, D. and Studer, R. eds). pp. 372–387, Springer, Berlin
10. Rogerson, S. and Bynum, T.W. (1995) Cyberspace: the ethical frontier. In *The Times Higher Education Supplement.* 9 June 1995, http://www.timeshighereducation.co.uk/story.asp?storyCode=98490&sectioncode=26
11. Toffler, A. (1981) *Future Shock*. Bantam Books, New York
12. Nielsen, J. (2003) Web guru fights info pollution. BBC News Online. 13 October 2003, http://news.bbc.co.uk/2/hi/technology/3171376.stm
13. Evans, C. (1979) *The Mighty Micro: The Impact of the Computer Revolution*. Victor Gollancz, London