ICTs, Citizens and the State: Moral Philosophy and Development Practices

Tim Unwin
UNESCO Chair in ICT4D
Royal Holloway, University of London
September 2009

Not to be cited without the author’s permission
ICTs, Citizens and the State: Moral Philosophy and Development Practices

Tim Unwin

Abstract: This paper examines the moral implications of the use of ICTs in e-government initiatives, focusing especially on national databases, identity cards and surveillance technologies. It suggests that in resolving debates over these, we need to reach ethical resolutions concerning notions of trust, privacy and the law. It also draws attention to the ethical problems that emerge in linking the notion of Universal Human Rights with the introduction of ICTs in developing countries.

This paper explores the ways in which Information and Communication Technologies (ICTs) have been used in mediating relationships between states and citizens, focusing especially on their introduction in so-called ‘developing’ countries in the context of e-government initiatives. In particular it seeks to use arguments in moral philosophy to examine the rights and wrongs of such initiatives. The paper takes the form of an engagement with four key sets of literatures and arguments: recent studies in information ethics, typified by the collection of essays edited by Capurro et al. (2007) on African Information Ethics… (see also Floridi, 2001, 2009); popular arguments concerning the introduction of identity cards and the increased levels of state security monitoring, both in the UK (see for example http://www.no2id.net/, accessed 20 August 2009) and elsewhere, as exemplified in Freedom House’s (2009) assessment of Freedom on the Net; Raymond Geuss’s (2008) recent Philosophy and Real Politics, which asserts that philosophers need to understand the real reasons why political actors behave as they do, focusing especially on notions of power, concepts and motives; and European traditions of political philosophy, particularly deriving from John Locke’s Two Treatises of Government (1987) and Thomas Hobbes (1996) Leviathan.
These issues are of critical contemporary importance for three main reasons. First, e-government initiatives have been widely advocated by international organisations for implementation in ‘developing’ countries, and are generally seen as being inherently ‘good’ (Guida, and Crow, 2009); there is a dearth of literature exploring the many negative implications of such initiatives. Second, many of the more popular debates pertaining to the use of ICTs by states have focused primarily on economic arguments, as with debates over the costs of introducing identity cards into the UK; insufficient attention has focused on the fundamental moral principles that underlie the changes in relationships between states and citizens caused by such initiatives. Third, the implications of such changes for moral philosophy itself need to be examined. In essence, it is important to understand not only what our existing ways of deciding what is right and wrong have to tell us about the role of ICTs in mediating between states and individuals, but also what those mediations themselves have to tell us about our traditional ways of deciding what may be better or worse.

Such an adventure faces huge challenges at its commencement, in large part because of the contested nature of the terrain that it will encounter. In particular, there is little agreement about the definitions of that terrain. Geuss, (2008, p.6) has, for example, recently provided a strident critique of the notion that ‘politics is applied ethics’, challenging the view that we should ‘start thinking about the human social world by trying to get what is sometimes called an “ideal theory” of ethics’. For Geuss (2008), we cannot start by building our political philosophy on the initial identification of historically invariant principles, but rather we need to adopt a realist stance in which we begin by examining how institutions actually operate in a given society rather than with how people ought to act in some ideal way. Geuss’s (2008) arguments are explored further below, but are introduced here primarily to emphasise that there are significant problems with traditional European notions of ethics, derived largely from the universalist and rational agency arguments of Kant, that suggest that ethics should focus first on the identification of an ideal theory on which we should act, and then on the application of such a theory to the actions of particular people. While I wish to
start this analysis with an exploration of how we might begin to structure an argument around ideal ethical principles, I conclude that in practice we need to focus on the real impacts that the introduction of new ICTs have on the lives of different group of people, both within the world’s poorest countries, and also between them and all those living in richer countries.

In the first section, I argue that one of the problems in traversing this terrain is the plurality of meanings attributed to notions of ethics or moral philosophy in the current literature. Much recent literature adopts a very broad definition of ethics, as for example with many of the contributions to Capurro et al.’s (2007) edited volume on African Information Ethics, and yet other volumes on profoundly ethical issues, as with Freedom House’s (2009) report on Freedom on the Net, do not mention the word ‘ethics’ at all. Here, I therefore wish to adopt a quite focused definition of ethics and moral philosophy as systemic reflection on moral questions, with the emphasis being on the systematic. Likewise, I accept its usual fourfold division into descriptive ethics (descriptions of existing moral practices and beliefs), normative ethics (concerned with the solution of moral problems), meta-ethics (the examination of ethical reasoning itself) and applied ethics (how moral outcomes can be achieved in particular contexts) (Smith, 2000; Cohen and Wellman, 2005). Rather than focusing, as does much of the literature relating to ethics and ICTs, on descriptive and applied ethics, my main concerns are with meta-ethics and normative ethics. Fundamentally, I am interested in the contexts in which ethical arguments are being used in the literature on the implementation of ICTs in development practice, and in how we can tell what is good or bad, better or worse, in the application of these practices. The context in which I wish to address these issues is the way in which ICTs are being used to transform the relationships between states and individuals, focusing primarily on ‘developing’ countries.

---

1 Although it does refer fleetingly to such notions as public or common morality
2 The notions of ‘development’ and ‘developing countries’ are themselves hugely problematic, and open to wide-ranging interpretation. For a discussion of these issues explicitly with respect to ICT4D, see Unwin (2009)
Human Rights, Knowledge Societies and universal ideals

The increasingly prominent role played by new ICTs in social and economic change in the 1980s and 1990s (Castells, 2000) has been matched by the recent emergence of the distinctive fields of computer ethics and information ethics (see for example, Floridi, 2001, 2008, 2009). As Adam (2001, pp.235-6) has commented, ‘Over the last decade and more, considerable interest has developed in the topic of computer ethics, as a new area of enquiry, to the extent that it has been hailed as the most important recent development in the philosophy of ethics’ (see also Gorniak-Kocikowska, 1996). Likewise, Floridi (2001, p.3) has suggested that ‘Information Ethics is the new ecological ethics for the information environment. It argues that the digital divide can be bridged. What we need to do is to fight any kind of destruction, corruption, pollution, depletion (marked reduction in quantity, content, quality or value) or unjustified closure of the infosphere, what shall here be referred to as information entropy’.

Within the field of Information and Communication Technologies for Development (ICT4D) (Unwin, 2009), one of the reasons why ethics has become so prominent is that it was explicitly mentioned in the Geneva Declaration of Principles agreed at the first part of the World Summit on the Information Society (WSIS) in 2003. This asserted that

‘We acknowledge the importance of ethics for the Information Society, which should foster justice, and the dignity and worth of the human person. The widest possible protection should be accorded to the family and to enable it to play its crucial role in society’ (WSIS, 2003, para 57).

However, nowhere does this explicitly make clear what specifically is meant by ‘ethics for the Information Society’. Moreover, by juxtaposing mention of the ‘family’ with ‘ethics’, it suggests that it is the family that should be the key unit of ethical consideration, rather than, say, the ‘individual’ or the ‘community’. 
Two years later, the Tunis Commitment, reiterated the WSIS commitment to ethics, noting that

‘We reaffirm our resolution in the quest to ensure that everyone can benefit from the opportunities that ICTs can offer, by recalling that governments, as well as private sector, civil society and the United Nations and other international organizations, should work together to:’

amongst other things

‘address the ethical dimensions of the Information Society’
(WSIS, 2005, para 9).

Again, this does not specifically indicate what is meant to be understood by ‘the ethical dimensions of the Information Society’, although earlier in the Commitment these appear to be laid out in the claim that

‘We reaffirm our desire and commitment to build a people-centred, inclusive and development-oriented Information Society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge, to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals.’

This is a remarkable assertion, suggesting as it does that for the first time in history a set of technologies, in this instance ICTs, can indeed be used to enable everyone to achieve their full potential. As such, it represents an ‘ideal’ theory or aspiration, rather than the ‘realist stance’ that Geuss (2008) would have us explore. More specifically, by linking the ethics of the Information Society directly to the Universal Declaration of Human Rights, it explicitly suggests that there are indeed universal human rights concerning these technologies.
However, this is nowhere justified, nor is the contested nature of universal human rights (An-Na‘im, 1992; Evans, 1998; Dunne and Wheeler, 1999) ever recognised. In particular, the close inter-linkages between the development of the so-called Information Society, and the concept of universal human rights is never clearly explicated or acknowledged. For example, the creation of an increasingly interconnected world through the use of ICTs, has enabled powerful interests to assert ever more effectively that their vision of human rights is indeed the one that is truly universal. The Vienna Declaration of 1993, designed in part to update and streamline global human rights protocols, thus frequently mentions the importance of effective information dissemination about human rights (UN, 1993), and although it does not specifically refer to the role of ICTs in such dissemination, the rapid expansion of Internet access and the Web in the ensuing 15 years has done much to cement this ideology. Of particular interest is what the Vienna Declaration has to say about information technology:

‘Everyone has the right to enjoy the benefits of scientific progress and its applications. The World Conference on Human Rights notes that certain advances, notably in the biomedical and life sciences as well as in information technology, may have potentially adverse consequences for the integrity, dignity and human rights of the individual, and calls for international cooperation to ensure that human rights and dignity are fully respected in this area of universal concern’ (UN, 1993, para 11).

This is of very considerable pertinence, because it recognises that ICTs, in the form of ‘information technology’, may not actually be benign, but can rather have adverse impact on human rights. This returns us once again to the realm of ethics: how do we judge whether such impacts are indeed good or bad?

The Universal Declaration of Human Rights itself was shaped in a particular context at the end of the 1939-45 War, one that was dominated by a north American vision born from a particular European tradition, despite the relatively broad based membership of the Commission that drafted the text
This is not to argue that the Universal Declaration of Human Rights has not had value, but it is to emphasise most emphatically that it is not universal, and should instead be seen as having emerged in a particular social, economic and political context. Put quite simply, I cannot accept the claim of the Vienna Declaration that ‘The universal nature of these rights and freedoms is beyond question’ (UN, 2003, para 1). Of considerable importance for the argument that follows, is the recognition that the declaration is one that is above all based on individual rights, rather than communal responsibilities. This has especial significance for my arguments relating to proprietary and communal or open software, as well as for the ways in which knowledge is interpreted as being either an individual benefit or a global common good.

Within the UN system, discussions over ethics and ICTs have been especially articulated by UNESCO, notably in the context of a shift of language from arguments relating to an ‘Information Society’ to discourses about a ‘Knowledge Society’ (UNESCO, 2005; see also World Bank Institute, 2007). As I have argued elsewhere (Unwin, 2009, p. 22), such discourses ‘place considerable emphasis on the notion of knowledge as a global public good, on the emphasis within knowledge societies of human rights agendas, and on the importance of knowledge sharing’. They specifically address ethical issues, but they have a problematic tendency to conflate the normative (what should be) with the positive (what is) (see also Britz et al., 2006). For example, the team writing UNESCO’s (2005, p. 18) volume entitled Towards Knowledge Societies argues that

‘A knowledge society should be able to integrate all its members and to promote new forms of solidarity involving both present and future generations. Nobody should be excluded from knowledge societies, where knowledge is a public good, available to each and every individual’.

---

3 Membership of the Commission consisted of representatives from Australia, Belgium, Byelorussian Soviet Socialist Republic, Chile, China, Cuba, Egypt, France, India, Iran, Lebanon, Panama, Philippines, United Kingdom, United States, Soviet Union, Uruguay and Yugoslavia
Four features should be noted about this claim: first, it is normative, suggesting what a knowledge society should be like; second, it focuses on individuals, rather than communities; third, it makes a positive claim that knowledge is a public good; and fourth, it seeks to be inter-generational by combining the interests of present and future generations. Its normative and inter-generational claims suggest again that it seeks to identify a universal ideal to which we should aspire. However this claim conforms neither to historical evidence nor to contemporary practice. As Britz et al. (2006) assert, ‘Africa still has a long way to go to become a true knowledge society’. While it is fine for agencies like UNESCO to make claims about what it would like the world ideally to be, there is also a need to recognise the harsh realities of the contemporary world in which the rich and powerful are seeking to control both information and knowledge for their own interests. In this context, Google can, for example, be seen both as being ‘good’, in the sense that at present it makes information freely available to people who have access to the Internet, but also ‘bad’ in the sense that it aspires to host as much information as possible on its servers, from which the company can then generate profits as a result of its monopoly position (Vise, 2005). As Arlidge (2007) has recently commented,

‘as it prepares to celebrate its 10th birthday, Google has developed serious engine trouble. A series of missteps have left it facing claims that it has gone from a benign project – creating the first free, open-all-hours global library – to the information society’s most determined Big Brother. It stands accused of plotting some sinister link between its computers and us: that it wants, somehow, to plug us into its giant mainframe – as imagined in The Matrix or Terminator.’

One of the fundamental problems with UNESCO’s (2005) claims about knowledge societies is therefore the suggestion that knowledge is, rather than should be, a global common good (UNESCO, 2005, p.18). While agreeing that ‘information is in many cases a commodity’ (UNESCO, 2005, p.19), the authors still wishes to maintain an ideal that knowledge can somehow
transcend the commodifying power of capital. As Habermas (1978) has argued so convincingly, different forms of knowledge have always had different interests associated with them, and there seems little evidence that the introduction of new ICTs has changed this. Indeed, as explored further below, it can be suggested instead that ICTs have actually created new ways through which powerful interests can exploit knowledge to their own benefit, as also in the example of Google above. Paradoxically, this does seem to be admitted by UNESCO (2005, p.22) in their comment that ‘knowledge itself has become “commoditised” in the form of exchangeable and codifiable information’. Rather than being a global common good, the positive reality is that knowledge is currently becoming increasingly commoditised in the service of particular interests. As Roberts (2000, p.439) has so cogently commented, ‘As one element in a broader neo-liberal discourse, where the primacy of the market for organising all human activity is taken for granted, “knowledge” becomes just another commodity: something to be bought, sold, traded and consumed’. Should anyone be left in any doubt about this, one need only look to the increasing costs being levied on university students in many countries of the world, primarily on the grounds that the knowledge they will gain through their education will enable them to earn more in their subsequent careers. As Lord Mandelson, the UK’s Secretary of State for Business, Innovation and Skills, which from 2009 also has responsibility for Higher Education, commented in July 2009 in the context of university funding and student fees, ‘A university education remains the gateway to the professions and a ticket to higher lifetime earnings on average’ (http://www.bis.gov.uk/mandelson-universities-are-central-to-the-economy-and-social-mobility). Such an argument should never be used as justification for people to pay for access to a global common good, knowledge. Education, scholarship and learning are about far more than simply earning more income in one’s subsequent career.

Ethics and ICTs in a ‘development’ context

In a discussion on the Kenyan ICT Action Network in July 2009, Edith Adera drew attention to the following observation about Pakistan’s National Database and Registration Authority:
‘...Pakistan has created a national smart ID card database, managed by the National Database and Registration Authority (NADRA). Currently this database holds 170 million fingerprints, 72 million facial images, and has already issued 70 million ID cards. The information stored within the system is used for highway toll collection, cash grant systems, national drivers license system, civil registrations, passport and visa issuing, passport insurance and control biometric refugee registration, and the ID cards and access control system for the Pakistani army. The mere scale of this database raises questions about access management, security, and interoperability, but these have yet to be answered. A centralised pool of information may be an invaluable tool to any government; especially one trying to raise its people out of poverty. But given how high the stakes are, we need to ask ourselves whether adopting a one-sided approach and focusing on the benefits alone will not harm those same people in the long run’.

Once again, this forces us to address fundamental questions about how and why such schemes have been introduced, and in particular the need to explore the negative impacts as well as the positive benefits. As she commented in introducing this article, ‘Wonder what Kenya is planning. Worth a debate?’.

One of the most comprehensive accounts of ethical issues surrounding the use of ICTs in a development context has been Capurro et al.’s (2007) edited collection on African Information Ethics in the Context of the Global Information Society, which forms the proceedings of the first African Information Ethics Conference held in Pretoria. This conference was inspired by the WSIS (2003) Geneva Declaration, and under the patronage of UNESCO it was intended to address the ethical challenges of the information society within Africa, with one of its outcomes being the Tshwane Declaration on information ethics in Africa (http://icie.zkm.de/TshwaneDeclaration,
In introducing the proceedings, Capurro (2007) observes that not much has yet been published on the impact of ICTs on African societies and cultures from a philosophical perspective. He goes on to draw a distinction between information ethics for Africa, and information ethics from Africa, suggesting both that ethical considerations are important so as ‘to avoid the digital gap within African societies’ (Capurro, 2007, p.10), and also that we need to explore works by Africans on philosophy so as better to understand effective ways in which African solutions to ethical questions about the introduction of ICTs can be implemented. In particular, he stresses the importance of African oral traditions, and the role that communal concepts such as ubuntu play in the African context. As he argues, ‘personal privacy – being a key ethical value in Western countries – might be considered as less important from an Ubuntu-based perspective, even if we accept that there are several conceptions of privacy in both the West and East’. This again reinforces the relevance of the distinction already made between the ‘individual’ and the ‘communal’ when considering ethical implications of the introduction of new ICTs.

In reviewing the processes giving rise to the Tshwane Declaration, Frohmann (2007) highlights the way in which the declaration largely repeats existing dogma on information ethics. As he argues, ‘African information ethics is treated as a plug-in to a system of stable phenomena already assembled together in a fixed totality by’ the ‘three absolute and already stabilized virtues’ of universal human values, human rights and social justice (Frohmann, 2007, p. 137). He is also highly critical of the process that gave rise to this declaration, noting that ‘the Declaration reflects the political reality of the Tshwane Conference, where instead of pursuing scholarly discussion of ethics in any philosophical sense the academic delegates were set the task of crafting a document – the Tshwane Declaration – only to find that none of their recommendations survived the final draft’ (Frohmann, 2007, p.138). For Frohmann (2007) scholarly discourse on ethics was replaced by a process of shaping moral codes relating to the installation of information technologies in Africa. He goes on to argue that
‘Language that envisions African service to a taken-for-granted reality – the global information society – recalls for even moderately critical readers the analyses of critical global political economists who have labored to show that the primary advantages of such bureaucratization and service accrue to the owners and developers of those information systems who along with other corporate giants have long recognized the public relations value of installing ethical modules in their organizational structures’ (Frohmann, 2007, p.138)

My question is fundamentally about whether these structures actually derive benefit for the poor and marginalised communities that they are meant to, or whether instead they merely serve to reinforce the interests of global capital? To me, the ethically interesting dimension of this question concerns how we make such a decision. This force us to address another equally important issue, since it is not necessarily simply an either/or, good/bad choice, but rather a matter of whether the two may in fact be compatible, and if so whether sufficient benefit may accrue to the poorest, despite the ‘corporate giants’ and their direct beneficiaries becoming more powerful and financially better off. How do we decide if it is acceptable for the digital divide and thus relative poverty to increase, even though many poor and marginalised people are indeed better able to lead fulfilled lives as a result of the introduction of new ICTs? Again, this comes back to the distinction that Geuss (2008) makes between a political philosophy that focuses on ideal theories and one that addresses contemporary political reality.

In seeking to respond to some of these issues, Frohmann (2007, p.141) uses Deleuze’s concept of agencement (Deleuze and Guattari, 1987), usually translated as ‘assemblages’, particularly as developed in the work of Latour (2005), to suggest that ‘Multiplicity and heterogeneity, not uniformity and universality, generate the intensities needed to build assemblages’. Using Nabudere’s (2005) work as an example, he shows how
‘universalist conceptions of human rights actually interact in specific cases with cultural diversity and identity in Africa – an antagonism found on an abstract level in UN documents espousing both universal human rights and ethical imperatives to defend cultural diversity – ‘ and that this ‘demonstrates the value of approaching human rights not as stabilized states of affairs applied in the manner of universal standards but as assemblages territorialized and reterritorialized in particular sites’ (Frohmann, 2007, p.141)

In order to pursue some of these ethical ideas further, and to try to address the questions raised earlier about Pakistan’s National Database and Registration Authority, the next section therefore focuses down on three specific aspects of e-government, namely the use of national databases, identity cards and surveillance technologies.

**e-Government in the context of national databases, biometric identify cards and surveillance.**

One of the outcomes of the expansion of interest in the ways in which ICTs can be used in development practice has been a rapid increase in the implementation of e-government policies and strategies across Africa, Asia and Latin America (Heeks, 2001, 2006; Heeks and Santos, 2009; Hanna, 2008; Guida and Crow, 2009). Much of this interest has, however, focused on technological solutions and the ways in which e-government can be made more effective, rather than on fundamental ethical dimensions surrounding the negative and positive aspects of the introduction of such systems. Heeks’ (2001) seminal work on e-governance, for example, merely mentions ethical considerations once, and then only *en passim*; his more recent authoritative book on *Implementing and Managing eGovernment* (Heeks, 2006) likewise focuses primarily on finding ways to improve e-government, and makes little explicit mention of moral and ethical questions about the inherent nature of e-government. To take another example, the UN’s (2008) latest *e-Government
Survey makes no mention at all of ethics or morals in its 225 pages of text. In this context, it is salient to note that Heeks’ (2001, p.3) list of the five main benefits that ICTs can bring to governance, namely that it is cheaper, does more, is quicker, works better and is innovative, make no mention of such issues as whether or not it is fairer or more just. For Heeks (2001, p.4) e-governance thus focuses on improving government processes, connecting citizens and building interactions with and within civil society, rather than with issues of justness and rectitude.

While most work on e-government does indeed still tend to concentrate on the delivery of services by governments through digital technologies to citizens, businesses and other organisations (see for example, UN, 2008), more recent approaches to e-governance have placed more emphasis on its transformatory role in shaping the relationships between governments and citizens. As Guida and Crow (2009, p.284) note, the term is increasingly being used to describe ‘the goals and potential, however elusive, of utilising the transformational nature of technology to create a more open, fair and empowered society which is actively engaged in the process of being governed’.

E-Government and e-Governance are fundamentally to do with changes in the relationships between states and citizens, and as with any technological intervention they can have both positive and negative effects. If the positive benefits have in the past been given most prominence, highlighted by those seeking to promulgate and benefit from e-government initiatives, there is now a growing body of evidence that is emphasising their negative attributes. Karlekar and Cook (2009, p.1), for example, note that ‘As the internet and other new media come to dominate the flow of news and information around the world, governments have responded with measures to control, regulate, and censor the content of blogs, websites, and text messages’. They argue that it is not only in what they describe as ‘some of the world’s most repressive regimes, like China and India’, but also in ‘more

4 Although one footnote does indeed mention a reference to a paper on ethical dilemmas in the creation of global classrooms.
democratic countries - such as the United Kingdom, Brazil and Turkey' where internet freedom is increasingly being undermined; as they conclude, ‘On the whole, threats to internet freedom are growing and have become more diverse, both in the array of countries that impose restrictions and in the range of methods employed’ (Karlekar and Cook, 2009, p.1).

At this stage, it is useful to stress three important aspects of e-government. First, it is generally a top down process, decided upon and implemented by governments. Moreover, in the case of developing countries, such decisions are usually heavily influenced by the policies of international agencies and donors (see for example, UNDP (http://ictd.undp.org/e-gov/, accessed 25 August 2009). It is hard to find any e-government initiatives actually being driven by the citizens that they are meant to serve. Second, despite the increasingly globalised character of ICTs, and their ability almost instantaneously to bring people together from many different parts of the world, much of the regulation pertaining to such things as use of the internet is actually at a national scale. As the examples cited above from Freedom on the Net (Freedom House, 2009) illustrate, much e-government activity is therefore actually about the ways in which the governments of nation states seek to restrict or protect, depending on your point of view, their peoples from external influences. It is also salient here to note that there is actually little new in this, with the Cold War from 1945-91 also being a period when ICTs, mostly in the form of television and radio technologies, were used by states either to promote their messages, or to block incoming messages from their enemies. E-government is thus fundamentally about ways in which ruling elites can use ICTs to retain their power. A third important aspect of many e-government initiatives in developing countries is their association with explicit attempts to enhance so-called democracy (Korac-Kakabadse and Korac-Kakabadse, 2001), and to impose a particular kind of government structure. This is yet another example of the universalising tendency of the current global system of power, where the world’s richer countries, such as the USA and the states of Europe are seeking to impose their own model of governance on the rest of the world through institutional structures such as the United Nations. The trouble with this is that, as David Held (1995, 2006)
has so lucidly explained, there are actually many different kinds of democracy, and it is therefore difficult to determine exactly which aspects of democracy it is that ICTs are intended to support.

Bearing these three observations in mind, it is helpful to explore how e-government issues were considered in the context of the discourses presented at the Africa Information Ethics Conference in 2007 (Capurro et al., 2007). E-government was one of the four specific themes addressed under Topic 2: cultural diversity and globalization (Capurro, 2007), and this linkage with globalisation is in itself significant given the comments above on the way in which the implementation of e-government programmes in developing countries has been closely intertwined with a global rhetoric about democratic values. Three papers focused explicitly on aspects of e-government and e-governance (Carbo, 2007; Ngulube, 2007; Onyancha, 2007), but none of them really addressed the fundamental ethical questions relating to the impact of e-government on the relationships between states and individuals with which the present paper is concerned. Onyancha (2007), for example, in reviewing African government websites, makes the following recommendations in a concluding section on ‘ethical issues’: that government websites should be published in several languages; that governments should formulate policies relating to the right to access and free access to information; that there should be clarity of administrative responsibility with governments clearly stating their ownership of their websites; and that there should be single government portals rather a multiplicity of websites owned by different government departments. The ethical implications of such normative recommendations are not, though, explored in any detail. Likewise, Ngulube (2007) refers primarily to the problems faced in implementing e-government initiatives in Africa, particularly relating to infrastructure, infostructure, and education. Whilst there are indeed ethical questions that can be asked about why access to infrastructure varies so markedly across Africa, these are not really addressed in his paper. Finally, although Carbo (2007) does draw attention to the importance of human rights, dignity and trust in the practices of governments and to the importance of issues surrounding privacy, their ethical dimensions are again, insufficiently investigated.
In order therefore to explore such ethical issues in more detail, and in particular the debates over privacy that were touched on by Cardo (2007), I turn now to a brief consideration of ethical questions raised by the use of ICTs in national databases, biometric identity cards and surveillance. My intention is to explore how the ethical dimensions of such usage are constructed, so as to provide some insights into the ways in which we might be able to make judgements as to the rights and wrongs of government usage of ICTs for particular ends. Just because one can indeed now perform certain government functions in new and innovative ways through the use of ICTs, does not necessarily mean that governments should actually seek to do so. The challenge is to identify the grounds upon which we can make rational decisions about this, and thus answer the question raised earlier in this paper about the desirability of the NADRA database in Pakistan.

The dearth of publications, or indeed popular discourse, about ethical dimensions of the introduction of these three aspects of e-government in developing countries is significant (although see Mason, 2004). Whilst there are numerous reports of the ‘roll-out’ of such technologies in different parts of the world (Saxby, 2005; Anon, 2006; Anon, 2007), most of these focus almost exclusively on their technical or economic aspects, and are usually written from a broadly positive perspective. Much can, though, be learned about the possible ethical implications of these technologies from the debates and discussions, both academic and popular (see for example the work of the members of European Digital Rights, http://www.edri.org, the UK’s NO2ID campaign http://www.no2id.net and the Open Rights Group http://www.openrightsgroup.org, accessed 26th August 2009), in more affluent parts of the world (see Burbridge and Maguire, 2009; Fuchs, 2009; Poullet, 2009; Stol et al., 2009; Sullivan, 2009), and especially in the case of the UK, where the government has recently published its Digital Britain report (BIS, 2009). Indeed, the UK makes a particularly good case study for two main reasons: first, because unlike many other parts of Europe its citizens do not yet have to have identity cards, and therefore the debates associated with their introduction are just as appropriate there as they are in developing
countries which are also considering their introduction; and then also because Britain has increasingly been described as a ‘surveillance society’, with estimates in 2006 suggesting that it then had more Close Circuit TV (CCTV) cameras per head of population (14) than any other country in the world (Wood, 2006). Interestingly, in this context, the Digital Britain report makes no mention of the words ‘ethics’, ‘moral’ or ‘ethical’, and focuses very much on the practical aspects of implementing a digital society. The Prime Minister, Gordon Brown’s eulogistic introduction to the report summarises its intent:

‘Only a Digital Britain can unlock the imagination and creativity that will secure for us and our children the highly skills jobs of the future. Only a Digital Britain will secure the wonders of an information revolution that could transform every part of our lives. Only a Digital Britain will enable us to demonstrate the vision and dynamism that we have to shape the future’ (BIS, 2009, p.7).

The drivers for this are clear: economic success, an increase in the number of jobs, and an innovative future. As the text goes on to say, the report’s ambition is ‘to secure the UK’s position as one of the world’s leading digital knowledge economies’ (BIS, 2009, p.7). The potential dangers, the downsides and the ethical issues that this ambition raises are rarely considered, apart from in the context of digital security and safety in Chapter 7 where even then it is discussed largely in terms of its economic aspects rather than the ethical questions that it raises.

Some of the more important claims that have been raised about each of these aspects of e-government are listed below (Tables 1-3). Many are contradictory, but they are summarised here primarily to highlight the complexity and diversity of ethical issues that need to be addressed when e-government initiatives are introduced into countries in the developing world.
Table 1

**National Database of Citizens**

*Positive*

- For governments
  - Enables easier checking of individual identities and life histories
  - Enables cheaper delivery of services, although cost models are controversial
  - Increases efficiency of managing citizen control, especially of ‘criminals’
  - Provides a means to reduce ‘illegal’ immigration
  - Centralises existing diverse sources of information about citizens
  - Means of managing the rapid increase in the amount of information available about citizens (especially relating to tax and illegal activities)
  - Can reduce number of civil servants in government departments, in part through outsourcing

- For citizens
  - Enables swifter access to information
  - Facilitates agencies in accessing their life histories for medical reasons
  - Individual benefits (in terms of financial/tax and personal safety) gained from government delivery of more efficient and cost effective services

*Negative*

- For governments
  - Costs of managing such a database are large, albeit balanced by potential savings in labour
  - Potential concerns over image as ‘Big Brother’ controlling agency
  - Risks of ‘enemy’ or ‘criminal’ access to information about citizens
  - May not have the capacity satisfactorily to analyse the data available

- For citizens
  - Raises questions about what information a state can legitimately keep about its citizens
  - Possibility that agencies of the state could use data to make false claims about an individual
  - Increased potential of identify theft through unauthorised access
  - Difficulties of changing any errors on the database
### Table 2

**Biometric Identity Cards**

**Positive**

- For governments
  - Helps to guarantee transparency and reliability of electoral processes
  - Prevents illegal activities and threats (claims that it reduces terrorism, illegal immigration, under-age drinking and criminal activity)
  - Increases ability to monitor movement of citizens
- For citizens
  - Simplifies proof of identity for purposes such as banking, health, insurance
  - Reduces identity fraud
  - Enables foreign national working in a state to have proof of identity
  - Facilitating travel to other states that recognise the identity card

**Negative**

- For governments
  - Costs of implementation and management
  - Potential failure of untried technologies
  - Risks of fraudulent use of counterfeit ID cards, as with banknotes and passports
- For citizens
  - States do not currently have the right to have access to biometric information about citizens; why should they?
  - Makes identity only proven through the presence of the ID card, rather than through trust in personal physical identity
  - Increases the potential of identify fraud
  - Ultimately, citizens have to pay for ID cards, either through taxation or directly
  - Could be used to restrict access
  - Increases potential for citizens to be subject to acts of violence against them by states or agencies thereof
  - Loss of ID cards would create significant levels of inconvenience for citizens
  - Passports currently enable freedom of travel; no need for IDs
  - Prevents individuals having multiple identities
### Digital Surveillance (CCTV, digital communications)

**Positive**
- For governments
  - Facilitates monitoring and control of citizens: CCTV for crowds; e-mail, Internet and ‘phones for correspondence and networking.
  - Reduces potential violent and illegal activities, or at least leads to their relocation.
  - Facilitates transport management.
  - Provides evidence for use in criminal proceedings.
  - Ability to control use of digital media, including the restriction of ‘illegal’ activities.
- For citizens
  - Enables swifter delivery of services in emergencies.
  - Reduces crime and increases sense of security.

**Negative**
- For governments
  - Costs of implementation and management of monitoring process.
  - Negative impression of appearing as overly controlling and ‘snooping’.
  - Potential increase in unsafe convictions as a result of flawed judicial processes.
- For citizens
  - States have traditionally been permitted to monitor when there is suspicion of guilt; monitoring of entire populations can thus be construed as implying guilt in advance.
  - Need to pay for state’s implementation of digital security systems either through taxation or directly.
  - Increased threat of others witnessing ‘private’ acts, particularly in terms of social relationships, and subsequent potential for such things as blackmail.
  - Emotional impact on state employees of witnessing certain disturbing events.
  - Lack of ‘ownership of correspondence’: traditional letters were ‘sealed’ and only usually legally read by the recipient, but with digital communications they could be read by anyone.
  - Increased potential for centrally stored communications or images to be ‘hacked’.
  - Increased possibility of guilt by association in criminal proceedings.
Two initial observations can be made about these summaries. The first concerns the way they have been constructed, suggesting dichotomies between ‘states’ and ‘citizens’, and between ‘positive’ and ‘negative’. This was deliberate, since this is often how the arguments are portrayed, as their proponents seek to justify their positions based upon some contrasting intuitive universal ideal ethics. However, the reality is actually much more complex than this. Even taking an ideal stance, the interests of governments and citizens should be synonymous, and thus what is good for governments should be good for their citizens. That it is possible to consider something being ‘good’ for a government, but ‘bad’, or at least not so good, for its citizens, therefore already suggests that there are significant concerns over the ways in which such technologies may be using by states. This has been highlighted by Karlekar and Cook (2009) in their survey of freedom on the Internet, where they note that both democratic governments (which are generally seen as being ‘good’) and oppressive regimes (generally seen as ‘bad’) are increasingly seeking to control the Internet. In so doing, they draw attention to both negative trends (expanding forms of censorship, privatization of censorship, lack of transparency and accountability, legal threats, and technical attacks) and positive ones (poverty not being a barrier to new media freedoms, growing civic activism, and Internet freedom being greater than press freedom). However, a key point to reflect on is that most of these observations could actually be seen as being either positive or negative depending on the position from which one is standing.

A second key observation is the dominance of economic arguments in the debates over these three aspects of e-government. Whilst there is not the space here to go into this in detail, it is highly salient to note that although much of the opposition to identity cards and a national database in the UK was indeed based on certain key moral principles, it was actually the economic arguments, notably the cost of implementing such systems, that appear to have been of most importance in changing the views of the government during the mid- to late-2000s. Young (2009) thus notes that in a recent parliamentary debate opposition parties focused primarily on concerns
over the level of funding of ID cards, even though they were also ideologically opposed to them. As he concludes, these costs include the following existing and likely contracts:

- ‘Thales UK was awarded an £18m, three-year contract to manufacture and deliver the first ID cards to students and volunteers, starting this autumn.
- IBM has been awarded a £265m deal to build the biometrics database to support ID cards and passports.
- CSC has been given a £385m deal to upgrade the application and enrolment system – applicable to passports and ID cards.
- A £400m contract to deliver the next generation of UK biometric passports went to smartcard specialist De La Rue.
- A contract for a case management system for the UK Border Agency – again applicable to both passports and ID cards – worth “substantially less” than £500m is still to be awarded.
- A mooted £500m contract for production of the cards themselves has not yet been awarded and is likely to be delayed until after the next General Election’ (Young, 2009).

These figures emphasise once more the considerable value of such contracts and the financial burden that the introduction of e-government initiatives into the world’s poorer countries places on their governments. Ultimately, it raises the question of who benefits most from such initiatives: governments, citizens, or the global corporations that develop and implement these technologies?

In trying to resolve these issues, three long-standing ethical debates are of direct relevance, namely those relating to trust, privacy, and the law. The final section of this paper briefly discuss the importance of these principles in the context of e-government initiatives in developing countries, and in so doing draws on some of the foundations of political philosophy.
Trust, privacy and the law: governments and citizens

Drawing both on their own practical experiences of political turmoil in 17th century England and France, as well as their intuitive capacities, Thomas Hobbes (1651) and John Locke (1689) formulated many of the foundations of the social contract theory that still underlies much contemporary political practice in so-called democratic countries across the world. In essence, Hobbes argued in *Leviathan* that in striving to unite their desires for peace and power, men cede some of their individual rights to a sovereign in return for protection. For Hobbes, people are equal in nature but are always restless for power. In order to avoid war, they therefore give away some of their rights, so that they can go about their daily lives, and indeed ‘industry’, in peace. Locke likewise acknowledged that people would agree to form a state to protect their property and lives, but he was only prepared to give the state authority if it helped to achieve greater common good. He argued strongly that where this was not the case, people had both a right and a duty to replace the ruler. While there have been many subsequent developments and critiques of these positions, two fundamental aspects of this formulation of social contract theory still seem relevant today in helping to explore the ethics of e-government.

First, there is the suggestion that individual people give something up to the state in return for specific benefits from that state. This seems to be particularly important in understanding the idea that individuals in a democracy might be willing freely to give up aspects of their privacy in return for greater benefits, such as more security or more efficient delivery of services. The challenge of course is whether this will actually happen in the context of e-government. One of the reasons for the debate over identity cards and national databases is thus quite simply that people are becoming less willing to give up aspects of their privacy because they do not trust the government to deliver on the supposed benefits. This is scarcely surprising, when governments make excessive claims about the potential benefits of

---

5 This itself is highly problematic, because it implies that ‘in their natural state’ individuals have rights that they can indeed give away. It also raises fundamental questions about the relationships between individuals and communities, and thus on the rights and responsibilities debate discussed earlier in this paper.
these technologies. In reporting on the debates over UK Identity Cards, Ford (2005) thus noted that ‘The Government has admitted that it has overplayed the advantages of identity cards. Tony McNulty, the minister in charge of the ID card project, admitted that ministers had been too enthusiastic in suggesting that the cards could be the answer to a host of problems such as terrorism and multimillion-pound benefit fraud’.

Second, and related to this, Locke’s arguments about the need to replace unjust governments remains of paramount importance. It is here that the two sided character of many information and communication technologies comes into play. On the one hand, ICTs can indeed be used by governments to control and restrict their citizens, but the anarchic aspects of the Web, social networking technologies, and mobile telephony can all be used to hold governments to account and indeed potentially to lead to their overthrow. In 2009, the violence surrounding the elections in Iran was thus widely reported on mobile ‘phones and by local bloggers (http://unwin.wordpress.com/2009/06/21/updates-on-iran/, accessed 26th August 2009), and as I write the Internet is being used by the Camp for Climate Action to organise the ‘swoop starting points’ where their actions would take place in London, thereby enabling people to come together without the police knowing the locations in advance (http://www.climatecamp.org.uk/actions/london-2009/swoop, accessed 26th September 2009). Significantly, despite the anarchic potential of these digital technologies, the balance of power still seems to be with state authorities, as so sadly revealed by the failure of the ICT-enhanced protests in Burma in September 2007 (although for a more positive view from the African context, see Heacock, 2009).

These comments highlight once again the importance of ethical issues relating to trust, privacy and the law, each of which has its own long history of debate. In bringing this paper towards its conclusion, it is important to draw attention to some of the particularly pertinent aspects of these histories for understanding the ethical dimensions of e-government initiatives in developing countries.
Trust

Trust is essential to effective human relationships, and has attracted a wide diversity of interpretations. Sonnenberg (1993, p.23), for example, has commented that ‘Trust is the fabric that binds us together, creating an orderly, civilised society from chaos and anarchy’. Much literature in the last two decades has focused especially on business ethics, and the importance of establishing clear and coherent regulatory environments and ethical guidelines upon which business, professional activities and government practices should be implemented. As Kramer (2009, p.69) has thus noted, ‘For the past two decades, trust has been touted as the all-powerful lubricant that keeps the economic wheels turning and greases the right connections – all to our collective benefit’. However, as he goes on to point out, recent corporate scandals, and especially the global financial meltdown of 2008, have forced many people to ask ‘Is there perhaps a problem with how we trust?’ (Kramer, 2009, p.70).

Traditionally, approaches to trust have tended to focus on both social and psychological explanations (see for example, Baier, 1986; Coleman, 1990; Misztal, 1996). There is thus a particularly interesting moral dimension to matters of trust, because those whom societies might describe as being immoral, such as many criminals, can themselves still engage in trusting one another. Theoretically, therefore, it is conceivable that an immoral government could still be trusted by the majority of its people, just in the same way that groups of criminals might also trust each other. In the context of ICTs, Gerck’s (1998) work has been particularly influential, building on the notion that ‘trust is that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel’. Significantly, Gerck (1998) argues explicitly that trust is not ‘surveillance, auditing, reputation, authorization, closed-loop control, insurability, indemnifiability, belief, accountability, hope, intuition, faith, unqualified, the inverse of risk, the absence of risk, transitive, distributive (in psychological, sociological and legal sense), associative (in mathematical sense; also in psychological, sociological and legal sense), symmetric’. For the present
discussion of e-government initiatives, and the example of surveillance noted above, this would therefore suggest that the use of surveillance indicates that governments do not trust citizens. However, it is not quite as simple as this, because if the notion of ‘citizens’ is then subdivided into those that are trustworthy (the majority) and those that are not (‘criminals’ or ‘terrorists’) then governments can still claim that surveillance is used to protect the former from the latter. Nevertheless, for this to be acceptable, citizens still need to trust governments, and it is a failure in this relationship that has been of most significance in recent debates over e-government. Where citizens do not trust governments, no amount of e-government will encourage the delivery of better governance, however that may be defined. Indeed, the growing challenges to the digital surveillance approaches adopted by governments across the world, are but one factor that may actually be contributing to an increased lack of trust citizens have of their governments. Paradoxically, the use of digital technologies may actually be reducing the trust between citizens and governments rather than increasing it as intended and expected.

Following Gerck’s (1998) definition, trust cannot be transferred through ICTs, but it is essential for their effective use. Hence, governments and citizens need to enter trust relationships distinct from those involved in the use of ICTs for any form of e-government to be used effectively. No amount of e-government technology, for example, will actually make a government change its attitudes and approaches towards its citizens, unless that government has in the first instance decided to adopt new ethical stances towards such concepts as transparency, equity and fairness. As Guida and Crow (2009, p.285) have thus commented

‘Concurrent with growing acceptance of the potential of technology has come the realisation that the human side of technology-based government initiatives – the social engineering issues associated with changing how civil servants approach their jobs, how citizens view their roles in the governing process, and how and when partnerships to deliver government services involving business or not-
for-profit organisations should be utilised – is where the most vexing challenges lie’

Such arguments are of the utmost importance in the context of developing countries, and suggest three important conclusions for the implementation of e-government programmes:

• If e-government initiatives are to benefit citizens, they must be based on pre-existing relationships of trust between governments and citizens;
• All else being equal, the introduction of e-government programmes is most likely to reinforce existing relationships of power, rather than change them
• Relationships of trust between citizens and governments can be facilitated by the creation of effective regulatory bodies and coherent ethical guidelines, but these often themselves reflect existing power relationships, and some form of external international mediation may well therefore be necessary for their effective implementation.

Privacy
As with trust, there has been extensive recent debate over the ethics of privacy, and although there have been considerable discussion of privacy issues relating to the introduction of identity cards and national databases in the richer countries of the world, much less attention has been paid to these in the context of developing countries. The benefits of digital identities, as with the use of digital technologies in elections (Heacock, 2009), have all too often been lauded, with insufficient attention being given to their potential negative effects. As Jim Killock, executive director of the Open Rights Group, has argue, ‘Governments tend to think that gathering new information on citizens is a good thing. But that’s not true if our privacy is undermined and our data isn’t secure. We need to see privacy by design: you can’t bolt on privacy at the end of big government IT projects, we need privacy safeguards built into systems right at the start’ (http://news.bbc.co.uk/1/hi/uk_politics/7872425.stm, accessed 3 September 2009).
This does though, beg a fundamental question as to what privacy actually is. One view is that privacy is merely a good that can be weighed up along with any other goods. As Etzioni (2005, p.254) has commented idealist questions about privacy are often false because they are posed as being cost free, whereas actually people weigh up different costs and consider actions in the light of their various benefits:

‘The same people who want to have more privacy often use their credit and debit cards leaving a trail that tells what they purchased at Victoria’s Secret and with whom they checked into a motel or with whom they flew to a beach resort. Even if these people are reminded that if they pay cash then their privacy will be much better protected, most of htem will show you in the way they conduct their affairs that they would rather do with much less privacy than be even slightly inconvenienced’.

Etzioni (2005, p.241) goes on to note that privacy as a legal right is actually something quite new, and even in the USA, the Fourth Amendment to the Constitution limits privacy in cases where the needs of the community over-ride it: ‘It outlaws only unreasonable searches’. For Etzioni (2005, p.260), privacy is but one right among many other often incompatible ones, and ‘we must constantly weight how much importance we ought to accord privacy, and how much importance we ought to accord other values, above all, the protection of our families, communities, and homeland’. According to such arguments, it is therefore indeed appropriate for governments to introduce new measures to protect citizens and communities, even if some limitations on individual privacy are introduced. To do so, though, governments have to indicate that external situations have changed in order to legitimate such actions. In the case of the UK and USA, the introduction of many new digital technologies, such as ID cards and national digital databases, has thus been justified in terms of their potential and efficacy in reducing the likelihood of terrorist attacks.

In contrast, and adopting a more idealist stance, there are arguments that suggest that ‘privacy gives each of us more control over our own life –
which on average, if not in every case, is likely to lead to a freer world’ (Friedman, 2005, p.264). From this perspective, the way in which governments wield power is particularly significant. Generally, governments have more power than individual citizens, and thus the more a government knows about each citizen, the easier it is for them to implement such power. However, as Friedman (2005, p.265) again comments, ‘Reducing government’s ability to do bad things to us, at the cost of limiting its ability to protect us from bad things done to us by ourselves or by other people, may not be such a bad deal’. This is particularly significant in terms of the use of ICTs, because these have already greatly facilitated the ease with which others (governments or indeed other citizens) can access information about people. If governments and their agents can be trusted to be good, this might not matter if the benefit is that we can all live more peaceful lives, but there are two fundamental problems with this:

- Not all governments really serve the interests of all of their citizens, and
- Even where they do, there is no guarantee that future governments will adopt the same approaches to use of data that has already been gathered.

One extreme view of the future proposed by Brin (1998) is that ultimately there will be a fully transparent society in which not only can governments watch their citizens, but citizens can also watch governments completely transparently. Even if we do not achieve such a vision, though, as Friedman (2005) points out, there is an important asymmetry in this, because governments can arrest citizens, whereas citizens cannot arrest governments.

Ultimately, discussions of privacy in the context of ICT4Dc and e-government initiatives come down to three basic questions:

- whether citizens will ultimately benefit sufficiently from the loss of privacy that might entail, to compensate for their loss of privacy;
- whether governments have in place sufficient mechanisms to ensure (a) that they, or their agents, do not abuse the information that they have about people, and (b) that other citizens are prevented from accessing such information; and
• whether the overall communal benefits of such e-government systems outweigh the sum of losses of individual privacy and freedom?

This last issue returns us once again to the issues raised earlier in this paper about the possible differences in ethical implications and contexts between African communal models of society, and the currently more dominant north American and European models based fundamentally on individualism. Accordingly, it could be argued that loss of individual privacy may actually be less of an issue in African contexts than it is in north American and European societies. Although this is a logical conclusion from such arguments, it is an issue that requires much further exploration and debate.

Ethics, Law and Human Rights
The relationships between governments and their citizens are fundamentally conditioned by the legal systems that they have in place. It is these laws that specify what individual citizens are not permitted to do, and what a society’s agreed penalties are for failure to abide by them. It is these laws that provide the context for specifying what an individual’s rights are. There are, though, various different legal systems in operation across the world, and so it is of crucial importance that any e-government initiative takes into consideration the legal context within which it is intended to operate. Even in European and north American societies, there are two fundamentally different approaches to these matters.

On the one hand, states such as France and the USA have a legal system based on a codified constitution, often based on or associated with a bill of rights. The actual term ‘bill of rights’ was first used to refer to a bill passed by the British Parliament in 1689, but other better known examples include the declaration of the rights of man and of the citizen in France in 1789, and the United States Bill of Rights completed in 1789 and ratified in 1791. In essence, such constitutional frameworks seek to ensure basic political, economic and social rights that governments agree to provide to their citizens, reinforced through the legal system. In contrast, legal systems in other states, notably those derived from common law practices in England, do
not have such a grounding in a formal constitution guaranteeing fundamental rights, but rather base judgements on statutes, case law and convention. Above all, they are based on precedent. In any e-government initiative, the ethical implications of the specific legal means through which individual rights are supposed to be guaranteed, need to be considered in determining the appropriateness of the proposed intervention at the interface between state and citizen.

Most legislative systems have adopted Locke’s fundamental constitutional principle that the individual can do anything apart from that which is prohibited by law, whereas the state may only do things that are explicitly authorised by law (Locke, 1987, *The Second Treatise*, Chapter 9, Section 124). One area where tensions can arise, though, is at the interface between national and international law with respect to human rights, especially since most ICTs are fundamentally interconnected at a global, rather than national, level. A particular state, with one legal system may have very different intentions and mechanisms for maintaining what it sees as the rights of its citizens compared with those of another state with a different legal system and intentions. Hence, since the middle of the 20th century, a growing amount of international legislation, particularly promulgated through the UN system, has sought to promulgate and enforce international human rights, namely those that are seen as universal. Currently, since 2005, it has been the UN Human Rights Council that has the mandate to investigate violations of human rights (http://www2.ohchr.org/english/bodies/hrcouncil/, accessed 4th September 2009). Significantly here, the UNHCR has played an important role, for example, in supporting other agencies in ensuring that ICTs have been included in human rights conventions. Thus the 2008 Convention on the Rights of Persons with Disabilities (http://www.un.org/disabilities/default.asp?navid=12&pid=150, accessed 4th September 2009) for the first time includes ICT accessibility as an integral part of accessibility rights (Leblois, 2008).

Locke’s important constitutional principle, though, raises fundamental ethical dilemmas, particularly at times of rapid technological change. It
becomes essential for the legal system, notoriously slow in its deliberations, to move swiftly to be able to adjudicate on entirely new agendas that have usually not been considered in the founding constitutions at the heart of constitutional law, or the precedents determining the practice of common law. Put simply, if some use of ICTs has not yet been defined as illegal, citizens are allowed to act with impunity, yet states should have to seek authorisation from the courts to be able to implement a new ICT based initiative, such as the construction of a national database of citizen information. If the above discussion on privacy suggested that the balance of power in the use of ICTs is usually with governments, it is thus here within the legal and jurisdictional realm that it can be seen to shift back somewhat to the citizen. However, this is only in circumstances where the legal system is indeed independent from the legislature.

This is of particular importance in the context of e-government initiatives in developing countries because all too often these legal and ethical dimensions are insufficiently considered. The introduction of ICT-based technical solutions, for example through health or education management information systems, or through national voter databases using biodata, are seen as offering sufficient inherent advantages that their legal and ethical implications are either ignored or simply not considered.

Conclusions: beyond human rights
This exploration has primarily focused on shedding light on some of the all too often hidden ethical dimensions of the implementation of e-governance initiatives, especially in developing countries. Two main initial conclusions can be drawn. First, there are indeed many complex ethical aspects associated with such initiatives, and while to date the emphasis among governments of developing countries, international agencies and donors has very largely been on their positive practical benefits, this paper calls for much more thorough attention to be paid to their ethical grounding, and especially to the balance of rights and interests between citizens and the state. Second, in so doing, I suggest that three areas warrant particular attention, namely the
ethics of trust, privacy and the law. This paper has only begun to sketch out some of the implications of such a consideration, and has deliberately sought to place emphasis on the types of question that need to be asked by citizens in developing countries when such initiatives are being advocated. It is here that Geuss’s (2008) emphasis on existing real political contexts, rather than the imposition of some external ideal ethical solution, needs to reiterated. The fundamental point I wish to emphasise is that in each country where e-government initiatives are introduced, people need to ask about the rights and wrongs of such proposals in terms of existing ethical understandings of trust, privacy and the law.

However, over and above these two conclusions, such an exploration has highlighted three other related areas of particular interest and concern: the relevance of human rights; the balance of interests between individuals and communities; and the real interests that underlie the introduction of such e-government initiatives. First, this paper has raised fundamental questions concerning the continuing validity of much of the human rights based policy and legislation that has dominated global agendas during the last 50 years. We need to open up for sensible debate the value of such an emphasis on human rights, criticism of which is all too often seen as being politically incorrect and a taboo subject. Interest in human rights is often seen as lying at the root of 17th century English political philosophy derived from Hobbes and Locke, which in turn was of particular significance in influencing French thought culminating in the 1789 Declaration of the Rights of Man and of the Citizen. Hobbes (1996, p.87) thus argued that

‘From this fundamental law of nature, by which men are commanded to endeavour peace, is derived this second law; that a man be willing, when others are so too, as far-forth, as for peace, and defence of himself he shall think necessary, to lay down this right to all things: and be contented with so much liberty against other men, as he would allow other men against himself’.

However, if people do not actually have ‘rights’ that they can give up to a state, then we need to reconsider the whole edifice upon which such
arguments are built. It is perfectly understandable that following the horrors
of the holocaust in the early 1940s, many of the world’s leaders wanted to
establish some kind of basis for trying to prevent such atrocities happening
again, but it is salient to note that the subsequent declarations and
agreements on human rights have significantly failed to do this, as
massacres in places such as former Yugoslavia, Rwanda and Cambodia in
the 20th century so clearly indicate. An idealistic belief that people have
universal rights has not been any protection for those who have suffered at
the hands of those who do not believe in such rights. There is therefore a
strong argument that we need to shift the balance away from rights, and
towards the responsibilities that people and states have for each other. For
example, rather than simply claiming that knowledge is some kind of human
right, it would be a much more positive step to argue that states have a
responsibility to enable their citizens to gain knowledge. The same logic
applies to e-government. If we do not actually have rights to, for example,
our biodata, we cannot give up such non-existent rights to the state; the
counter to this is that we can also refuse to give our biodata to the state if the
state asks us to do so. We need a completely different basis for rationalising
the relationships between states and individuals.

There is a growing body of argument that suggests that rights based
approaches to development have failed to deliver on their promises, typified
by the International Policy Network’s (2009) recent publication on Fake Aid,
which concludes that

‘The research presented in this paper has questioned the
wisdom of DfID’s rights-based approach to international
development. We have argue, largely on the basis of
DfID’s own research and documents, that the approach
does not appear to have results ni an improvement of the
condition of the poor. Furthermore, substantial amounts of
funding predicated on the rights-based approach appear
to have been spent on projects that have little if any
connection even to the promotion of the “rights” of people
in poor countries’. 
The use of ICTs in e-government initiatives, and claims that access to knowledge is a human right thus raise fundamental questions about the nature of human rights, and how we should best seek to reduce poverty. I suggest here that greater emphasis on the responsibilities of individuals and states towards poor people rather than the purported idealised rights of individuals, might lead to more effective development practices.

Such arguments are closely allied with the balance in approaches to e-government based on the needs and interests of individuals and of communities. The contemporary hegemonic view that the elimination of poverty can be achieved through economic growth, places considerable emphasis on enabling individuals to fulfil their potential, rather than on the creation of successful and harmonious communities. Individuals are to be enabled to be effective producers, and thus also consumers, in a world economy that is forever growing. ICTs play a critical role in such a vision, not only enabling the world to be increasingly ‘joined up’ and thus for economic activity to take place faster, but also with the ICT sector being an engine of that growth in its own right. Until recently much of this ICT focus has, though, been on the individual rather than on the community. Proprietary software has dominated over Free and Open Source Software; individual content development and knowledge acquisition still dominates over Open Educational Resources. Evans (1998b, p.2) has emphasised that ‘At the centre of all human rights talk is the cardinal role given to the individual, both as a claimant and violator of rights’. If we began instead to focus more on responsibilities and on the roles of communities in e-government, rather than just the relationship between individual citizens and a centralised state, we might uncover some interesting new potential modalities for the effective use of ICT in enabling poor and marginalised communities to gain greater control over the futures. This returns us to the arguments of Capurro (2007) noted earlier, that ‘Western’ concepts of individual privacy are very different from the
‘African’ emphasis on communal traditions. It may well therefore be that many of the existing models of e-government developed around European and north America notions of individual privacy may be inappropriate in an African context, and that instead Africans should instead be designing new such initiatives around their own traditions and cultural practices.

Finally, these arguments lead to fundamental questions about why such e-government initiatives have been advocated so prominently for developing countries, and who has benefited most from their introduction. As Evans (1998b, p.2) has again noted, ‘any assessment of the dominant idea of human rights must include an analysis of interests, power and hegemony’. The ‘failure to explain the disjuncture between the theory and practice of human rights reveals that the literature has much to say about utopian visions and legal solutions but little to say about the social and political context in which violations take place’. Whatever the benefits to states, individuals and communities of e-government initiatives, there is no doubt that global corporations developing the hardware and software for such systems have been very great beneficiaries. Indeed, the efforts they have spent on working ‘in partnership’ with UN bodies, in influencing international development agendas, and in developing close relationships with governments in both the richer and poorer countries of the world, have led to rich financial rewards as they roll out their products to an increasingly unquestioning audience. The really difficult ethical questions that arise from this are about how we judge whether it is better for poor and marginalised communities for such e-government initiatives to have been introduced, or whether they might actually be more advantaged if their governments did not spend vast sums of money on their implementation. Just because it is possible to implement national citizen databases, to use biodata for ID cards, and to introduce sophisticated digital surveillance mechanisms does not mean that it is right to do so.

Let me conclude by returning to Geuss’s (2008) challenging arguments about philosophy and real politics. He concludes with the assertion that ‘modern politics is importantly about power, its acquisition, distribution, and
use’ (Geuss, 2008, p.96). One of the tasks for those of us concerned with the interface between politics and moral philosophy, is thus to explore the ways in which such power is played out in different social and cultural contexts. It is thus incumbent on us to raise challenging questions about the benefits and disbenefits of the introduction of e-government initiatives in developing countries, and to give voice to the voiceless, powerless poor. Furthermore, as Geuss (2008, p.69) has also argued, a statement such as “All individuals obviously have rights; let’s see what follows from this” is not a good starting point for philosophical reflection’. In this paper, I have tried to explore the realities of the introduction of e-government projects in developing countries, and in so doing to raise some ethical questions about them that I have found insufficiently addressed in much of the contemporary literature. I hope by so doing, that those who are themselves living through the implementation of such initiatives will be able to answer the questions and thereby enjoy fairer and more equitable lives.

References


Baier, (1986) Trust and antitrust, Ethics, 96(2) 231-60.

BIS (Department for Business Innovation and Skills) Digital Britain Final Report, London: Department for Business Innovation and Skills.


in Response to a Request from the Office of the High Commissioner on
Human Rights REFERENCE: IW/MK/SW/is, G3ict.
Locke, J. *Two Treatises of Government*, edited Ashcraft, R. (1987), London:
Allen and Unwin 320.5 LOC/A CHECK.
, accessed 25 August 2009)
Onyancha, O.B. (200&) E-governance in eastern and southern Africa: a
webometric study of the governments’ websites, *International Review of
Saxby, S. (2005) News and comment on recent developments from around
Edinburgh: Edinburgh University Press.
Law and Security Report*, 21(3), 251-62


