Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society

Siani Pearson

Strong Accountability and its Contribution to Trustworthy Data Handling in the Information Society

Siani Pearson (orcid.org/0000-0003-3576-9402)

Malvern, UK
siani.pearson@btinternet.com

Abstract. Accountability has long been the subject of discussion within public administration. Especially given the potential privacy and security risks arising from rapidly changing usage of information technology (IT), it can be useful to apply this notion also in the commercial world, relating to the actions of private organisations. However, accountability may be neither a necessary nor a sufficient condition for trust. In order to provide an improved basis for trustworthiness via enhancing accountability, certain conditions need to be met. In this paper we elucidate what these conditions are and explain the related notion and importance of strong accountability. Further, we ground this analysis within the wider context of organisational ethical decision making. As a topical case in point we focus on the data protection area and the protection of personal data.

Keywords: Accountability, Data Protection, Ethics, Trust

1 Introduction

Recent changes in information technology (IT) such as the shift to hybrid computing, increase in mobile connectivity and big data explosion are giving rise to a rapid transformation of enterprise IT. Adopting the new style of IT across all industry sectors has distributed our data everywhere, increasingly connecting different types of objects, collecting data in new ways, creating new exposures and attack surfaces. Concerns continue to grow around what has been called the 'darker side' of the Information Society.

From a societal perspective, this new IT can be used in ways that undermine social values and citizens' expectations [1]. Not only the privacy of the world's citizens is challenged, but there are unprecedented implications for their safety, for example concerning the reliability of critical infrastructure. The relationship between online privacy and security is actually quite complex, but online privacy goes beyond just confidentiality and encompasses a range of personal data handling mechanisms. There is a major difference between protecting data and using data, and in the past privacy and security have too often been considered as a zero sum gain. This tension between privacy and security that was discussed in the 1990s has now given way to more complex tensions such as privacy and autonomy versus open data and the free flow of information. These

tensions have been exacerbated by highly publicised cases such as the Snowden revelations about mass surveillance by the United States (US) intelligence services, the Schrems vs Facebook ruling by the European Court of Justice which ruled the European Commission's US Safe Harbour decision to be invalid in view of the Snowden revelations and the US State Court ruling about Microsoft not having to reveal emails held in Dublin to the US Justice Department. Citizens tend to cooperate with corporate surveillance because it offers convenience, and submit to government surveillance because it promises protection, and the result is a mass surveillance society underpinned by the new IT [2].

From the business perspective, associated risk has to be managed in a way that takes account of increasingly sophisticated cyber-attacks as well as potentially costly and complex regulatory pressures. Organisations face a trust challenge in which innovation and potential customer and societal benefits have to be weighed against legal obligations and customer and societal expectations. Not only do they need to decide which actions to take, but they may need to justify those to others [3]. Several recent cases highlighted in the press illustrate how, in order to increase trust with their customers, certain corporations are trying to protect the privacy of their customers' data from unwanted government surveillance, or at least be as transparent about what is revealed as they can, even though they face legal constraints about what they can do or reveal [2,4], and governments are trying to counter this in the name of national security [2,5]. Yet new services and practices typically involve multiple parties, some of whom are invisible to the data subject (DS) (individual whose data is being processed), and often their rewarding potential is proportionate to the potential risks in terms of privacy. More and more this data processing drives new business intelligence, helping innovation of new services and products. Moreover, dynamic and fierce competition can bring business practices that have not been tested from a privacy or data protection side.

Due to the way these services and networks tend to be borderless, addressing concerns around security is not only a national priority but is inherently global, and traditional legal frameworks are struggling to cope [6]. A multitude of different regulatory approaches, variable interpretations and academic visions generate uncertainty, complexity and risks for both companies and DSs as it may become difficult to ensure efficient protection of people's private life as well as to comply with applicable national laws and frameworks. Due to technological development, data flows can be dynamically changing, fragmented and global. The data of a specific DS may move from one day to the other in different places and be split into chunks requiring processing by different entities in different places of the world. Data creation and collection is increasing exponentially, in ways that may or may not provide new or improved services for the benefit of the DSs involved. In dynamic contexts like cloud there are further problems due to potentially weak trust relationships with new providers and the time needed to set up contractual arrangements that allow transborder data flow of personal information [7].

In order to maintain social and commercial trust, ethical codes of practice can be used by organisations and these will have to forbid some uses of information technology that are legally compliant, commercially profitable, and technologically possible. As Angela Merkel [8] said in a speech influenced by her experience of being an object

of US surveillance, "*When we proceed as if the ends justify the means, when we do everything that is technologically possible, we damage trust; we sow mistrust. In the end there is less, not more security*." Damaging trust may also result in the end in less profit and economic growth, and missed opportunities for improvement of lives by novel technologies.

In this paper we consider this problem of trustworthy organisational behaviour in our modern world and some solutions to it, focussing on the role of accountability. The following section considers briefly a number of ethical issues arising from recent changes in IT. Section 3 shows how ethical decision making can vary according to the framework adopted and considers how substance might be introduced into this process. In Section 4 the potential role of accountability within this process is assessed, particularly with regards to the central aspect of companies being able to show that they are behaving in an ethical way. Furthermore, in Section 5 the way in which accountability can be used in such a context in order to increase the trustworthiness of organisations to other parties, and especially to citizens, is discussed, and a case is made for *strong accountability* in order to satisfy this need. This is an important aspect in countering potential organisational behaviour in using notions of accountability, ethical frameworks and trust as a smokescreen for actions that ultimately decrease or attack universal human rights or social norms, decrease privacy, increase surveillance and the like, or ultimately do not take enough account of the summation of individual citizens' interests as against the single corporate interest. Although we consider European data protection as a significant example throughout this paper, analogous arguments may well apply to other domains including environmental sustainability.

2 Ethical Issues Arising from Recent Changes in Information Technology

In this section we consider a number of ethical issues arising from recent changes in IT. Web 2.0 and the rise of social networks shifted the balance of generation of Internet content from service providers to users, and thereby blurred the distinction between the data controller (DC) (who determines the means and purposes of processing of personal data) and the DS. Furthermore, over time:

- metadata has become increasingly viewable as personal data
- de-anonymisation has been made much easier
- storage costs have decreased
- the dangers of profiling have become evident
- large-scale collection of personal data using opt out mechanisms has been carried out
- differences between legislation applying where the DC and DS are in different countries could cause difficulties or potential harm to either (particularly in the sense of solutions being either ineffective or difficult to implement).

Connected to these general trends, different social and ethical issues can be associated with specific business models and technologies [9]. For example:

- *cloud computing:* lack of control and transparency [10], increased risks due to delocalisation and subprocessing [7], changes in risk perception [11,12], fears about surveillance by foreign governments [13]
- *big data:* secondary usage of customers' data, unwanted profiling, potential discrimination, easier de-anonymisation and mining of information from social networks
- *mobile*: unwanted collection of personal and location information by apps and issues with the readability of privacy policies
- *internet of things (IoT):* increased surveillance and behavioural tracking, difficulties in obtaining consent and difficulties in providing remediability and redress

One way of approaching this topic (fitting especially well with the social and historical European context, although the values apply universally) is preservation of values of the Enlightenment. During the seventeenth and eighteenth centuries, groups of intellectuals and philosophers, such as the Lunar Society of Birmingham, held discussions that helped articulate the notion of individual rights, amongst other things. But are such values that have underpinned our modern, secular age now under threat? As Tim Berners Lee has been quick to point out, the Internet need not itself result in that, as it may support universality and new rights including access to the Internet [14]. In order to avoid sweeping away rights and values in our digital era that the classical enlightenment helped reinstate, we need a new type of governance in which we can avoid technological 'dark paths' and in which fairness and human autonomy and rights are important. Ethical behaviour and choices corresponding to this will help build trust.

Although some social norms may gradually evolve, when it comes to the real consequences and harms of privacy intrusion the concerns will be the same and protection will not be useless. They are in fact more useful than ever when we observe that new innovative business models such as the ones mentioned above become less obvious and understandable by DSs. More specifically, individuals' ethical judgements about the collection of personal data are distorted by a number of practical factors. Even if an individual is actively and willingly disclosing data, he/she may be doing so on the basis of a flawed, incomplete or misleading set of assumptions. So, fear and doubts are shaping perceptions and trust becomes a key requirement. As the Eurobarometer survey (June 2015) [15] found, protection of personal data remains a very important concern for citizens. For example, nine out of ten Europeans think that it is important for them to have the same rights and protection over their personal information, regardless of the country in which the public authority or private company offering the service is based, and 69% of people say their explicit approval should be required in all cases before their data is collected and processed [15].

In general, ethical issues in IT include the following [16]:

1. one should have *no surprises* about data usage, or put too much emphasis on legal rather than what is legitimate, or overly make use of exemptions
2. *ethical dilution* may occur for example because harm can be difficult to quantify (and it could be potential and not just physical or financial)
3. *different stakeholders* are involved who could have competing interests, be unequal in terms of influence, or speak different languages

4. there can be changing and *complex contexts* magnifying risks of re-identification, lack of consent and lack of transparency

After having considered in this section some social and ethical implications in the information society, next we look at how these are being addressed in the form of ethical frameworks, what the impact of this is on businesses and how organisations can take active steps that include being accountable.

3 Ethical Decision Making

In section 1, we introduced the organisational trust challenge in which innovation and potential societal benefits are balanced against societal expectations and legal obligations. The business context and risk appetite of the organisation will affect how much it wants to risk non-compliance and various forms of backlash from users and from supervisory authorities; there are a number of potential risks including reputational damage, business continuity impact and fines. In order to avoid getting the balance wrong, ethical frameworks have an important role to play, and this will be considered further in this section. As we shall see in later sections, privacy by design, accountability and security are all aspects that need to be taken into account when organisations deploy the resultant solutions, as well as embedding ethical decision making into their operations and culture.

3.1 Different Approaches to Ethics

Much more broadly than the IT domain, different ethical approaches can be taken. Broadly speaking, these divide into teleological approaches (an ethics of what is good – for example, utilitarianism) and deontological approaches (an ethics of what is right – for example, using Kant's categorical imperative) [17]. Depending on which ethical approach you take, you might get a different answer about what you should do. A teleological decision looks at the rightness of wrongness based on the results or the outcomes of the decision. A deontological decision instead considers the moral obligations and/or duties of the decision maker based on principles and rules of behaviour. More information about the various different sub-approaches and philosophers in such a taxonomy of commercial ethics is given in [17]. The ethical dimensions of productive organisations and commercial activities have been studied since the 1970s within the field of business ethics, and a number of different approaches can be taken corresponding to this, as summarised for example within [18], ranging from Milton Friedman's [19] view of corporate executives' responsibility generally being to maximise profits while conforming to basic rules of the society to the opposing idea of corporate social responsibility (actions by businesses that are not legally required and intended to benefit other parties) [20].

3.2 Ethical Frameworks

In order to use these ethical approaches in a practical perspective by embedding ethics within business operations, one approach is to try alternative approaches and see the extent to which there is agreement.

This may look simple, but actually it is not necessarily an easy process. Let us consider comparing just one form of deontological judgment with one form of teleological judgment. If the result were that you would be doing the wrong thing and getting the wrong results (poor outcome), it might seem fairly obvious that a project fitting in that category should not go ahead, just as it needs little thought that a project doing the right thing and getting a good outcome is perfectly fine to go ahead. However, if you regularly deliver highly on the deontological spectrum but poorly on the teleological spectrum, you may well go out of business as it just might not be sustainable financially to continue. Conversely, if delivering highly on the teleological spectrum but low on the deontological spectrum, the drive for profit is taking precedence over consideration about what is (or is not) the right thing to do. In particular there is a zone of ethical nuances (especially along the boundaries between these) where the conclusion is not clear. Furthermore, when there is an economic slump, things can be perceived to be ethically questionable that would not have been before, so this ethical nuances zone can change [17].

Moreover, there tend to be different kinds of ethical perspectives for different types of organisations. For instance, guardian roles (such as regulators) seem to favour a deontological culture, whereas commercial institutions seem to favour a teleological culture and other actors (such as activists and technologists) may favour virtue ethics roles. Broadly speaking, governmental policy makers have outcome-based ethics, like commercial organisations, but are interested in economic and developmental outcomes at the national or regional level rather than the organisational level. Individuals who may be DSs have their own ethical framework. These different ethical frameworks and potentially conflicting objectives can make designing ethical codes of practice for the configuration and commercial use of new technologies difficult [17]. The code of practice could be a failure if it is unacceptable to any of these types of stakeholder. It must provide adequate protection of individuals' rights and interests. It must also give guidelines and assist with compliance to laws and regulations, as well as being practical for information technologists to comply with, and allowing new innovative mechanisms to achieve their potential for driving socially and economically beneficial applications.

In addition, as we considered in the previous section, it is beneficial to take into account a more nuanced understanding of "harm" including risk, potential harm, and forms of harm other than just physical and financial. In the data protection sphere, this is somewhat accounted for within the notion of Data Protection Impact Assessments (DPIAs) [3], which extend the standard practices of security risk analysis to examine also harms to the DS with regard to a proposed activity. In carrying out this assessment the summation of the harm across society needs to be properly evaluated and justified, as otherwise there is a risk that the potential harm to a single individual, as measured by an organisation that has a particular activity in mind, will typically tend to be overridden by other concerns.

3.3 Examples Addressing Technological Change

There are a range of different examples of ethical frameworks for decision making in contexts particularly influenced by recent technological development from different countries, most of which are still under development. In particular:

1. **British Computer Society (BCS) DIODE** [21]: a five stage ethical meta-framework (with iteration), within which different ethical approaches can be utilised.
2. **US Department of Homeland Security's Menlo Report** [22]: this framework for ethical guidelines for computer and information security research centres around four ethical principles: respect for persons; beneficience; justice; respect for law and public interest (which includes transparency and accountability).
3. **Information Accountability Foundation (IAF)'s Unified Ethical Frame for Big Data Analysis** [23]: an ethical framework for big data based on five values: beneficial; progressive; sustainable; respectful; fair.
4. **UK Government Cabinet Office's Data Science Ethical Framework** [24]: this focuses on six principles to stimulate ethical action when conducting data science: start with clear user need and public benefit; use data and tools which have the minimum intrusion necessary; create robust data science models; be alert to public perceptions; be as open and accountable as possible; keep data secure.
5. **European Data Protection Supervisor's (EDPS) opinions on ethics** [1,25,26]: freedom and dignity underpin the proposed approach, with user control, transparency, privacy by design and accountability being key aspects of the ethical solutions. In addition, EDPS has formed an ethics board to provide advice about ethical approaches to data protection in Europe.

Of course, there has been a substantial body of research in ethics for quite some time that is relevant to making ethical judgments relating to technology [17,27]. Of particular interest is a proposal by Gary Marx [28] that the ethics of a surveillance activity must be judged according to the means, context and conditions of data collection and the uses/goals. Furthermore, he has defined 29 questions related to this – the more one can answer these questions in a way that affirms the underlying principle, the more ethical the activity [28]. This provides a substantive basis for ethical judgment that appears to be currently lacking from many ethical frameworks – instead the latter often just present a number of key values as a basis for discussion by groups of experts and/or interested parties, and a process for the results to be reported back to other parties [23, 29].

Accountability is part of all of the above frameworks, but it is only one aspect of the proposed ethical code or approach. Other aspects that should be considered include for example: data minimisation; strong constraints around re-identification and (very) harmful uses of data; special treatment of sensitive data; constraints on sources used and recipients of data produced. Since this paper focuses on accountability, we will not consider those aspects further here. However, accountability is not only a way of ascribing ethical considerations beyond the DC, but also contributes to solutions: "*Transparency and accountability towards the range of stakeholders in business – including employees, customers, suppliers, shareholders, local communities, society at large and*

the environment – are both a standard that is expected, and a mechanism for securing compliance with codes of conduct designed to meet society's expectations." [30]. We consider this aspect further in the following sections.

Many ethical frameworks aim to take a wider range of aspects into account than just data protection [28]. However, in this paper, we will look in particular at one example that is a current hot topic, namely data protection.

European Data Protection. Security is a very strong requirement for data protection but it is not enough. The Organisation for Economic Co-operation and Development (OECD) privacy principles [31] have formed the basis for most data protection and privacy laws worldwide. These are privacy principles that should apply regardless of the institution or technology and are a rules-based (deontological) approach. Since the introduction of the legislative framework for protection of personal data in the European Union (EU) in 1995 (in the form of Directive 95/46/EC) which largely reflects these principles, there has been a fast pace of technological change. In 2003 this was complemented by the E-Privacy Directive (2002/58/EC), which, amongst other things, placed traffic and location data into the category of personal DS to the regime. As a result of further technological change (as discussed in section 2), there has been a major revision of European data protection legislation, called the General Data Protection Regulation (GDPR) [3], which was agreed upon by the European Parliament and Council in December 2015 and will introduce uniform requirements in all Member States, with the corresponding enforcement (and penalties of up to 4% of global turnover) starting in 2018. Within this regulation accountability is an important concept, that we now consider further.

4 How Accountability Can Contribute to these Solutions

4.1 The Concept of Accountability

Accepting responsibility, providing accounts and holding to account are central to what is meant by *accountability*. In the data protection context, the concept encompasses an end to end data stewardship regime in which the enterprise that collects personal and business confidential data is responsible and liable for how the data is shared and used, including onward transfer to and from third parties.

Accountability (for complying with measures that give effect to practices articulated in data protection guidelines) has been present in many core frameworks for privacy protection, starting with OECD's privacy principles in 1980 [31]. More recently, not only have regulators increasingly been requiring that companies prove they are accountable, but organisations themselves are seeing the benefits of taking an accountability-based approach. Legislative authorities have been developing frameworks such as the EU's Binding Corporate Rules [32] and APEC's Cross Border Privacy Rules [33] to try to provide a cohesive and more practical approach to data protection across

disparate regulatory systems, and these can be regarded as an operalisation of accountability.

From an analysis of the usage of the term 'accountability' in different fields [34], we propose the following definition:

Accountability: *State of accepting allocated responsibilities, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly. Responsibilities may be derived from law, social norms, agreements, organisational values and ethical obligations.*

Thus, accountability relationships reflect legal and business obligations, and also can encompass ethical attitudes of the parties involved. Our analysis actually combines and extends two aspects, based upon ideas coming from the social sciences [35] such that both commitment and enforcement are involved in accountability. Thus, the concept of accountability includes a normative aspect, whereby behaving in a responsible manner is perceived as a desirable quality and laid down in norms for the behaviour and conduct of actors. This can be applied to steer accountable behavior of actors *ex ante*. Accountability also encompasses institutional mechanisms in which an actor can be held to account by a forum, that involve an obligation to explain and justify conduct and ensure the possibility of giving account *ex post facto* (via accountability tools).

We broaden the notion of a forum to that of an accountee in a service provision chain, or more broadly a business ecosystem of interacting organisations and individuals − the actors of the ecosystem – who provide and consume IT-based services. These actors are controlled not only by internal factors of the system, such as codes of conduct and existing relations, but also by external factors such as regulations, the wider environment or even required skills.

Our approach is towards further operationalisation of the way accountability should be embedded in the ecosystem's norms, practices and supporting mechanisms and tools. First, we steer accountability behavior of actors including service providers *ex ante*. Second, we allow for a mechanism that entails the social relation between the accountor and accountee that involves an obligation to explain and justify conduct and ensures the possibility of giving account *ex post facto* (via accountability tools, such as the ones described in [36]).

Our model is that an *accountor* is accountable to an *accountee* for the following objects of accountability:

- **Norms**: the obligations and permissions that define data practices; these can be expressed in policies and they derive from legislation, contracts and ethics.
- **Behaviour**: the actual data processing behaviour of an organisation.
- **Compliance**: entails the comparison of an organisation's actual behaviour with the norms.

By the accountor exposing the norms it subscribes to and the things it actually does, an external agent can check compliance. For more analysis on accountability obligations, especially those owed by cloud service providers, and organisations that use cloud services, to regulators, stakeholders and society, see [6,36].

4.2 What Organisations Need to Do

Organisations operate under many norms, reflecting obligations and stakeholder expectations, and more broadly reflecting the various ethical, social and legal obligations that apply to their business situation. For example, in a cloud computing context, these could be regulations that apply to that organisation's provision or usage of cloud services (such as US Health Insurance Portability and Accountability Act, or HIPAA), as well as individual service level agreements (SLAs) that are in place. Accountable organisations need to implement appropriate measures to comply with these norms, which includes managing risks, adopting appropriate security controls, employing privacy by design and planning for remediation. Accountability does not typically itself directly address these requirements, other than providing information about mechanisms used or helping deal with breaches. In addition, a central part of accountability that increases transparency is to demonstrate how the norms are met and risks managed [30]. This risk assessment should include not only the standard organisational security risk assessment but also an assessment of the potential harm to individuals/DSs. It is possible indeed to incorporate the latter into the former or carry out a separate assessment (such as a DPIA or environmental assessment).

Accountability needs to be embedded into the culture and practices of the organisation. In moving to an accountability culture, decisions are made based on a set of ethics- and value-based criteria in addition to liability. So, for example, an organisation should not relocate operations to a country with a weaker legal framework in an effort to reduce its privacy protections.

The Global Accountability Project started by privacy regulators and privacy professionals [37] gives five essential elements of data protection accountability: (i) organisation commitment to accountability and adoption of internal policies consistent with external criteria, (ii) mechanisms to put privacy polities into effect, including tools, training and education, (iii) systems for internal ongoing oversight and assurance reviews and external verification, (iv) transparency and mechanisms for individual participation, and (v) means for remediation and external enforcement. Guidance has also been produced from Canada (and from other regulators around the world) about the expected form of comprehensive accountability programs that organisations should put in place [38]. In addition to such organisational practices, a variety of accountability tools may be utilised in support of accountability: see [36] for further details.

If these elements are already in place for data protection accountability, it makes sense to achieve accountability for ethical use of new technologies (such as big data collection and analysis) by extending the existing elements for data protection accountability to cover these considerations as well, so that the ethical code of practice is integrated into the existing elements. In any case, there should not just be a separate part of the organisation that deals with ethical issues, but the practices must be more integrated. For example, senior leadership should articulate and communicate an internal organisational policy consistent with the ethical code(s) and the policy should be part of mandatory data protection training for employees engaged in those activities and audited against.

Data Protection Example. The OECD principles [31] lead fairly directly to a number of practices that organisations acting as DCs need to take: organisations should be open about their policies and practices; personal information should only be collected for defined and relevant purposes; that information should only be used and disclosed in ways that are consistent with those purposes; access and correction rights should be granted to individuals; the data should be kept secure. However, there is a general movement globally towards less prescriptive approaches by regulators with organisations being allowed more control over which mechanisms to use, so long as they can show that they are meeting higher level goals [6]. In Europe, as mentioned in the previous section, GDPR [3] will include a new data protection principle: the principle of accountability. DCs will be compelled to adopt policies, organisational and technical measures to ensure and be able to demonstrate compliance with the legal framework.

5 The Relationship Between Accountability and Trust

Accountability can play an important role in enhancing trust in any information society; however, the relationship between the two concepts is complex because:

- *Accountability is not a necessary condition for trust*: deployment of certain security or privacy techniques (such as strong encryption with the keys controlled by the user) may engender trust without the need to trust the service provider, although trustworthiness is a much broader notion than security as it includes subjective criteria and experience, among other factors. It could be argued that if technologies were deployed where the trust model involves minimal trust in service providers and other associated actors – that is to say, if a combination of privacy enhancing techniques and encryption were used – there would be no need for accountability, and accountability is only needed to fill the gap where some trust in the service provider is needed.
- *Accountability may increase trust*: there is a paucity of such 'minimal trust' cases occurring in practice and indeed potential for re-anonymisation using additional information and meta-information even in such cases, thus creating a role for accountability. A good accountability deployment into an organisation might indeed increase its trustworthiness for potential clients: for example, a recent International Data Corporation survey [39] found accountability to be a key aspect of improving trust in cloud adoption.
- *Accountability is not a sufficient condition for trust*: it might be claimed that an accountability-based approach was being adopted, but this could be a smokescreen for weak privacy, perhaps even compounded by collusion in the verification process and the downplaying of DS expectations, wishes and involvement in the service provision. Indeed, verification is needed to encourage trust within an environment of market compliance, and trust issues will arise if levels of verification are perceived to be low.

From a societal perspective, an objection to accountability is that it could be a means to produce harmful effects for society [40]: big data and accountability can be regarded

as two cycles of policy manoeuvre to try to accomplish the abolition of purpose limitation in pseudonymous data [41]. This objection relates to the effects on both individual and society of a transition to continuous and ubiquitous data collection. Irrespective of the rules or algorithms governing how that data is used, this obviously would have legal effects on universal privacy rights, as well as a general "panoptic" effect of knowing that a record of individual behaviour exists inescapably. This is an entirely different social, political, and phenomenological situation that is incomparable with life without such (involuntary) life-logging.

Even if this wider context is ignored or disputed, other routes to potential harm to society, and DSs, may be considered. The trustworthiness of the process of verification of accounts produced *ex post facto* by that actor, and any associated remediation and penalties, are extremely important in affecting the strength of the accountability that evolves within a system. Moreover, there is a danger that individuals' viewpoints might be overlooked and their choice and control reduced.

In order to strengthen the link between accountability and trust by providing stronger grounds for trustworthiness, we argue for the notion of *strong accountability*, which encourages ethical characteristics (such as high transparency in balance with other interests) and trustworthy mechanisms for producing and verifying logs as well as adequate enforcement. In the following sections therefore we examine some ethical considerations associated with accountability, and then consider the nature of strong accountability itself.

5.1 Ethical Considerations

Accountability can provide trust in fair behaviour, detect issues when they occur and provide effective support for remediation while calling for explanation if something goes wrong. This latter aspect is discussed by Dubnick in relation to public administration and debates concerning responsibility and professional integrity, who summarises the discussion with: "*Ethical behaviour, in short, required the presence of external accountability mechanisms in all their various forms.*" [42]

Referring back to the discussion about accountability given within section 4.1, one aspect involves development of ethical guidelines for behaviour of actors, aimed at certain types of 'good willing' actors and reflecting best practice in stewardship of data. When it comes to protecting personal and confidential data, ethical principles such as 'do no harm' and 'respect for others' are clearly relevant. Yet in making a decision about what would be ethical, in some cases, the agents, actions or purpose might not be known, and possible results or outcomes might be highly uncertain. There are also a number of ethical principles that come into play arising from looking after valuable data. Personal data is often valuable to the person identified due to the harm that could come to that person if accessed, altered or anyhow misused by others. It is also valuable to an organisation for administrative purposes or for business activities. Confidential data has a value in terms of who may, or may not, have access to it.

With accountability as a mechanism [35], both good and bad actors are held to account for the consequences of their behaviour; following on from the discussion in section 3.2, the evaluators (and actors) might be using different ethical frames.

A number of ethical questions can also be posed with regard to the objects of accountability presented in 4.1:

Norms. How can legal obligations keep pace with developments in technology? How can ethical norms be defined and assessed? How can the interests of weaker parties not be subsumed by those of stronger parties? Is a given means of data collection ethically acceptable?

Behaviour. In determining whether the performance of an action by the accountor is ethical (and legal), there is a need to specify criteria for judging 'good', 'bad', 'right', etc., to judge the ethical quality of an accountor's actions according to these criteria, and provide reasons if there are shortcomings. A core part of accountability is to determine and clarify the rights and obligations of actors. To illustrate for a cloud service provision example, there is a corresponding need to clearly allocate privacy and security responsibilities across the various cloud supply chain actors. A closely related attribute of accountability is *responsibility* [43]: *the property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms*. There can also be a link with the ethical obligation to honour promises: personal and/or confidential data is given to a third party in exchange for some service, but only given on the premise (and condition) that the data given will be used in accordance with some agreement made between the data provider (whether it be a private individual, or a company) and the service provider, and that it will be adequately 'looked after'. Breaking an agreement or promise through a lack of care and attention could be unethical (based on Kant's Categorical Imperative). Agreements not met or broken promises lead to a breach of trust, a loss of trust and confidence in the organisation, and potentially an end to the working relationship.

Compliance. Form is important, in that the corresponding accounts provided by the accountor should be truthful. But what is an appropriate level of detail/content for a given context, and how can trust be provided in the verification process? Procedural ethics, in the form of the ethics of the reporting and enforcement process, is relevant here. There should be an element of dialogue and transparency without overwhelming the recipient. There should also be a willingness to admit error and to be honest about the facts and not bury bad news. In the account provision process, the focus is often on the consequences of behaviour (outcomes) but it might also take actions into account. Turelli and Floridi [44] put forward accountability as an ethical principle such that accountees must be capable of being aware of outcomes and able to know the 'actions' that led to the outcomes for which the accountor is responsible: "*an agent should be held accountable for the consequences of her/his actions or projects*". The accountor's story about the collection and use of other people's personal data must be open to inspection, rebuttal and dialogue by everyone because information privacy is a common, social and public good, not only an individual right [45].

In order to address how accountees might assess and enforce the interests of individuals and society, a notion of *democratic accountability* [46] can be useful. This reflects

the right of society to information about the extent to which a private organisation has complied with (minimum) standards of law and other regulation, as well as the right to information about public domain matters of a social and ethical nature (which can be elicited via public opinion). To restore power to the *demos* via democratic accountability, accounting arrangements are characterised by two essential elements that are core accountability attributes, namely transparency and responsiveness:

Transparency. This is a *property of a system, organisation or individual of demonstrating and/or providing visibility of its governing norms, behaviour and compliance of behaviour to the norms* [43]. Accountability implies a process of transparent interaction, in which the accountee seeks answers and possible rectification. In the data protection realm, the commitments of the DC need to be properly understood by the DS and others and the focus on transparency is mostly around the processes and procedures that the controller must implement to protect the data, rather than on the data as such. There is *ex post* transparency that informs about consequences if data already has been revealed (i.e. what data are processed by whom and whether the data processing is in conformance with negotiated or stated policies): for example giving an account of a data protection breach, with remediation options. But there is also *ex ante* transparency that should enable the anticipation of consequences before data are actually disclosed or processed (usually with the help of privacy policy statements). For example: does the organisation have an effective complaint handling process? Is there a responsible person, such as a chief privacy officer? Is there a privacy management framework? Is there staff training? In addition, transparency of operations helps counter the 'invisibility factor' [27], which is a key reason why computers raise ethical issues. For example, in cloud contexts data passes from the DS ultimately to a third party, where the location and involved processes may be invisible. Transparency is not however always a good idea because there are a number of tensions between transparency versus privacy, security, or usability – more information may lead to less understanding and may undermine trust [47]. In particular, there might be a conflict between maximal openness and the obligation to have appropriate technical and organisational security measures in place to protect personal data. Some of this conflict may be resolved by delegation of trust, in the sense that trusted third parties, such as auditors or supervisory authorities, may have privileged, yet verifiable, access to information that allows them to make assessments, of which only necessary information and conclusions are passed on to other parties (to avoid for example revealing specific security vulnerabilities or unnecessary personal data). This is in a sense a private accountability process, whereby there needs to be transparency between DCs and data processors, in such a way as to minimise security and privacy risks.

Responsiveness. This is a *property of a system, organisation or individual to take into account input from external stakeholders and respond to queries of these stakeholders* [43]. It could be argued that if the level of public and *ex-ante* accountability is not adequately high, there could be a lack of any role for individuals and public interest groups in the process, apart, maybe, for remediation mechanisms when negative impacts materialise. The provision of accounts is a process (see [48] for details) rather

than being static. Ethical considerations include: Is a dialogue invited for people involved indirectly, for example people for whom the action reported in the account is consequential (such as cloud subjects [36])? Are an organisation's ways of producing an account open to testing? How is a sceptical search for alternative explanations accommodated? What procedures are in place for resolving disputes between accounts?

5.2 The Need for Strong Accountability

In order to address the above issues, we argue that an accountability-based approach should have the following characteristics, which together support a strong accountability approach [50]:

- **Support for externally agreed data protection approach:** Accountability should be viewed as a means to an end (i.e. that organisations should be accountable for the personal and confidential information that they collect, store, process and disseminate), not as an alternative to reframing basic privacy principles or legal requirements. In this way, the accountability elements proposed within GDPR are instrumental to provide a certain assurance of compliance with the data protection principles, but do not replace them, and DPIAs, codes of conduct and certifications are proposed to increase trust in service providers who adhere to them.
- **Clarity of responsibility:** The commitments of the DC need to be well defined – this is (part of) the aspect of responsibility, that is an element of accountability. Service provider responsibilities should be defined in contracts and the definition of standard clauses by the industry, as validated by regulators, will help service users (such as cloud customers) with lower negotiation capabilities. The commitments of the DC should include all applicable legal obligations, together with any industry standards (forming part of the external criteria against which the organisation's policies are defined) and any other commitment made by the DC in privacy statements. In the cloud context, this is particularly important as entities may have multiple roles, e.g. they could be a joint controller and processor. Once again, the responsibilities of the entities along the service provision chain need to be clearly defined, including relative security responsibilities. On the other hand certain tasks will need to be jointly carried out to be effective, such as risk assessment and security management. In this case there is a clear need for cooperation and coordination.
- **Transparency:** This should be increased, in ways that do not decrease privacy or security. This includes the nature of accounts being public where possible, and the need for the commitments of the DC to be properly understood by the DSs (and other parties). In addition, the mechanisms used and relevant properties of the service providers in the provision chain need to be clarified as appropriate to cloud customers and regulators. Furthermore, DPIA/PIA is one form of verification for accountability (that should be used in conjunction with others) that can be used to help provide transparency about the nature of the risks, including the criteria used in the risk assessment, how decisions are made to mitigate risk, and whether the mechanisms to be used and implemented are appropriate for the context. Comprehensive obligations for controllers to inform supervisory authorities and DSs of personal data breaches

would further increase transparency. It is not only customers and end users that might be affected by certain kinds of data processing, but society at large. Transparency should therefore also be aimed at the general public and the regulator. This contributes to the maintenance of ethical standards, rather than stimulating a race to the bottom (of cost and privacy protection).

- **Trustworthy mechanisms for producing accountability evidence:** Trustworthy evidence needs to be produced and reflected in the account, for example using automated evidence gathering about non-compliance. Accountability evidence needs to be provided at a number of layers. At the organisational policies level, this would involve provision of evidence that the policies are appropriate for the context, which is typically what is done when privacy seals are issued. But this alone is rather weak; in addition, evidence can be provided about the measures, mechanisms and controls that are deployed and their configuration, to show that these are appropriate for the context. For higher risk situations continuous monitoring may be needed to provide evidence that what is claimed in the policies is actually being met in practice [49]; even if this is not sophisticated, some form of checking the operational running and feeding this back into an organisation's accountability management program in order to improve it is part of accountability practice.
- **Protection of evidence, assessments and accounts against tampering:** Technical security measures (such as open strong cryptography) can help prevent falsification of logs, and privacy-enhancing techniques and adequate access control should be used to protect personal information in logs and other accountability evidence [50]. Note, however, that data that is collected for accountability might be itself data that can be abused and hence also needs to be protected. The potential conflict of accountability with privacy is somewhat reduced as the focus in data protection is not on the accountability of DSs but rather of DCs, which need to be accountable towards DSs and trusted "intermediaries" such as the supervisory authorities.
- **Verifiability:** This is the extent to which it is possible to assess norm compliance [43]. Accounts must be adequately verified and collusion between the accountor, its partners and the accountee must be prevented. There needs to be a strong enough verification process to show the extent to which commitments have been fulfilled. Audits should be regular, in a similar way to Sarbenes-Oxley external audit, rather than one-off checks at the accountability programme level. Note however that missing evidence can pose a problem, and guarantees are needed about the integrity and authenticity of evidence supporting this verification and the account. In addition, the actor carrying out the verification checks needs to be trusted by the DS and to have the appropriate authority and resources to carry out spot checking and other ways of asking organisations to demonstrate accounts. That is why the data protection authorities will need to play a key role in the trust verification, for example in data protection certification. There are further related aspects supporting this approach in terms of responsibility and transparency, as listed above. In terms of external governance mechanisms, strong enforcement strategies, not only in terms of verification, but also in terms of increasing the likelihood of detection of unlawful practices and strong penalties if caught, seem to be a necessary part of accountability.

6 Conclusions

Accountability is not only an important aspect of ethical codes of conduct relating to business activities involving new technologies, but can also provide a mechanism for securing compliance with such codes of conduct. Centrally, it provides a mechanism for oversight within an organisation and enables external audit.

In the context of data protection accountability is particularly important, in that personal data has been given to an organisation for some stated purpose and it is expected by the provider of the data that it will be kept safe and used according to the established purposes. This is a legal obligation in many countries, and it is also a moral obligation. In our information society, personal data can be 'under the charge' of a variety of organisations in a way that is often not transparent or under the control of DSs, end users and customers. That data can also be transferred to many different locations under different legal jurisdictions.

In discussions about the laws that support data protection it is easy to get side-tracked from the most important issue. At the heart of data protection there is more than protection of the data – there is protection of the person to whom the data relates [3]. Transparency and accountability disclose satisfactory (or unsatisfactory) stewardship of data which to the originator – either DS or DC – is not just data but is information that has a value, either (for the DS) in terms of potential harm or possible benefit or (for the DC) through its business value or in costs incurred in collection and processing.

Enhancing accountability can be an improved basis for trustworthiness, and higher degrees of accountability, if appropriately advertised, could result in higher acceptance and trust by prospective customers. In order to be adopted, accountability must deliver effective solutions whilst avoiding where possible overly prescriptive or burdensome requirements. On the other hand accountability can also be used as a smokescreen for decreasing individual rights and for allowing businesses to give freer rein to non-paternalistic capitalist desires. The concept of 'strong accountability' is very important in helping demonstrate why (and indeed whether) an organisation should be trusted as well as in preventing the latter. An important aspect of this is that accountability should have democratic and ethical characteristics, in which transparency should be as high as possible in balance with other interests, and regulatory and supervisory authorities should have a primary role in the verification of the level of organisational compliance.

Acknowledgments. The author gratefully acknowledges input from Penny Duquenoy. It is partially based upon research carried out during EU A4Cloud project [51] and while employed at HPE Labs in Bristol, UK. However, it has been written subsequent to that period and does not represent any official position of HPE.

References

1. European Data Protection Supervisor (EDPS): Towards a New Digital Ethics. Opinion 4/2015. 11 September (2015)
2. Schneier, B: Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Co. (2015)

3. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016)
4. Ni Loideain, N.: EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. Media and Communication. **3:2** (2015) doi: 10.17645/mac.v3i2.297
5. UK Investigatory Powers Act (2016) https://www.gov.uk/government/collections/investigatory-powers-bill
6. Charlesworth, A., Pearson, S.: Developing Accountability-based Solutions for Data Privacy in the Cloud. Innovation, Special Issue: Privacy and Technology, European Journal of Social Science Research. **26:1**, 7-35, Taylor & Francis (2013)
7. Pearson, S.: Privacy, Security and Trust in Cloud Computing. *Privacy and Security for Cloud Computing.* S. Pearson and G. Yee (eds.), Computer Communications and Networks, Springer, 3-42 (2013)
8. Shae, M.: English translation of German Chancellor Angela Merkel's speech to the German Parliament, 29 January (2014)
9. UK Information Economy Council: Addressing consumer confidence in the Digital Economy (2015) http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/04/Information-Economy-Council-IEC-Principles-Consultation.pdf
10. Article 29 Data Protection Working Party: Opinion 05/2012 on Cloud Computing (2012)
11. Cloud Security Alliance (CSA): The Treacherous Twelve: Cloud Computing Top Threats in 2016, Top Threats Working Group (2016)
12. CSA: The Notorious Nine: Cloud Computing Top Threats in 2013. Top Threats Working Group, February (2013)
13. European Parliament (EP): Fighting Cyber Crime and Protecting Privacy in the Cloud. Directorate-General for Internal Policies (2012)
14. Berners-Lee, T., Halpin, H.: Defend the Web. In: Digital Enlightenment Yearbook. J. Bus, M. Crompton, M. Hildebrandt, G. Metakides (eds.), IOS Press, 3-12 (2012)
15. Jourova, V.: Data protection Eurobarometer. European Commission Factsheet 431 (2015)
16. Wilton, R.: Four ethical issues in online trust. In: CREDS 2014 (2014)
17. Harris, I: Commercial Ethics: Process or Outcome? Gresham Lecture, London, 6 Nov (2008)
18. Moriaty, J.: Business Ethics. Stanford Encyclopedia of Philosophy November (2016)
19. Friedman, M.: The Social Responsibility of Business is to Increase Its Profits. New York Times Magazine. September 13th (1970)
20. McWilliams, A., Siegel, D.: Corporate social responsibility: A theory of the firm perspective. Academy of Management Review. **26**, 117–127 (2001)
21. Harris, I., Jennings, R.C., Pullinger, D., Rogerson, S., Duquenoy, P.: Ethical Assessment of New Technologies: A Meta-Methodology. Journal of Information, Communication and Ethics in Society, **9:1**, 49-64, Emerald Group Publishing (2010)
22. Bailey, M., Dittrich, D., Kenneally, E., Maughan, D.: The Menlo Report. IEEE Security & Privacy, 71-75, March/April (2012)
23. Information Accountability Foundation: A Unified Ethical Frame for Big Data Analysis. Big Data Ethics Project, v1.0 (2014)
24. UK Cabinet Office: Data Science Ethical Framework. v1.0, 19 May (2016)
25. EPDS: Meeting the Challenges of Big Data. Opinion 7/2015. 19 November (2015)
26. EDPS: Opinion on coherent enforcement of fundamental rights in the age of big data. Opinion 8/2016. 23 September 2016 (2016)
27. Moor, J. H.: What is Computer Ethics? Metaphilosophy. **16**, 266-275 (1985)
28. Marx, G.T.: An Ethics for the New Surveillance. The Information Society. **14:3** (1998)

29. Raab, C.D.: Information Privacy: Ethics and Accountability, Keynote Presentation for the Expert Workshop on 'Cultures of Accountability', KU Leuven, 13 November (2014)
30. Lake, R.: Social Accountability, the OECD Guidelines for Multinational Enterprises and the OECD Principles of Corporate Governance. (1999)
31. Organization for Economic Cooperation and Development (OECD): Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
32. Information Commissioner's Office (ICO): Binding corporate rules. (2012)
33. APEC Data Privacy Sub-Group: Cross-border privacy enforcement arrangement. San Francisco (2011) http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf
34. Papanikolaou, N., Pearson, S.: A Cross-Disciplinary Review of the Concept of Accountability. In: Proc. TAFC. IFIP, May (2013)
35. Bovens, M.: Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. West European Politics. **33:5**, 946-967 (2010)
36. Pearson, S.: Accountability in Cloud Service Provision Ecosystems. In: Secure IT Systems. LNCS, vol 8788, Springer, pp. 3-24 (2014)
37. Center for Information Policy Leadership (CIPL): Accountability: A compendium for stakeholders. The Galway/Paris Project (2011)
38. Office of the Information and Privacy Commissioner for British Columbia: Getting Accountability Right with a Privacy Management Program. (2012)
39. International Data Corporation (IDC): Quantitative Estimates of the Demand of Cloud Computing in Europe (2012)
40. Bennett, C.J.: The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: Guagnin, D. et al. (eds.), Managing Privacy through Accountability, pp. 33-48, MacMillan (2012)
41. Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation. (2013)
42. Dubnick, M.J.: Accountability and Ethics: Reconsidering the Relationships. International Journal of Organization Theory and Behavior. **6:3**, 405-441 (2003)
43. Pearson, S.: Accountability in the Cloud. Proc. Trust in the Information Society, ITU Kaleidoscope Conference, Barcelona, Spain. 5-16, IEEE, 9-11 Dec (2015)
44. Turilli, M., Floridi, L.: The ethics of information transparency. Ethics Inf Technol. **11**, 105-112, Springer (2009)
45. Raab, C.: Privacy, Security and Safety: Intelligence Services and National Security, IFIP Summer School 2016, 'Privacy and Identity Management – Facing Up To Next Steps', Karlstad, Sweden, 21-26 August (2016)
46. Jaatun, M., Pearson, S., Gittler, F., Leenes, R., Niezen, M.: Enhancing Accountability in the Cloud. International Journal of Information Management, Pergamon (2016)
47. Tsoukas, H.: The Tyranny of Light. Futures. **29:9**, Elsevier Science, 827-843 (1997)
48. Gittler, F., Pearson, S.: Cloud Accountability Reference Architecture. D42.4a. A4Cloud Project Public Deliverable (2016) http://www.a4cloud.eu/sites/default/files/D42.4%20Reference%20Architecture%20%28Final%29.pdf
49. Pearson, S., Luna J., Reich, C.: Improving Cloud Assurance and Transparency through Accountability Mechanisms. In: S.Y. Zhu et al. (eds.), Guide to Security Assurance for Cloud Computing, CCN, Springer, Switzerland, pp. 139-169 (2015)
50. Butin, D., Chicote, M., Le Métayer, D.: Strong Accountability: Beyond Vague Promises. In: Gutwirth, S., Leenes, R., De Hert, P. (eds.) Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Springer, pp.343-369 (2014)
51. Pearson, S. et al.: Accountability for Cloud and Other Future Internet Services. In: Cloud Computing Technology and Science, pp. 629-632, IEEE (2012)