The Meaning of 'Accountability' in the Information Privacy Context

Charles Raab

University of Edinburgh

Abstract

'Accountability' is a term in good currency among regulators, business, and consultants in the world of information privacy protection. They are developing practical accountability approaches, and critical debate is well underway. The time is right therefore to look at the concept 'accountability' itself in terms of its meaning within the relationship among data controllers, other organisations, and the public. Such an examination involves considering what an 'account' is as an explanatory, communicative and evaluative performance, and how accountability relates to transparency and trust. This understanding will help in assessing whether the current development of the principle and practice of data protection accountability satisfactorily embodies these meanings, or needs greater precision in order to become truly effective.

Introduction: Accountability and Responsibility

There have been many innovations in the policy world of information privacy and data protection during the past 40 years. These range from the adoption of principles and guidelines, laws and Directives, codes of practice, privacy-enhancing technologies, 'privacy by design', binding corporate rules, standard contractual clauses, and perhaps other devices. Some innovations are of long duration, universal, respected, and implemented with varying success, while others are adopted by few and scorned by many, perhaps ultimately to be remembered only as fleeting presences on the fashion catwalks of regulatory history. We can only use informed guesswork about whether privacy is better protected through these measures, because such judgments are not easily amenable to quantification. However, gains can be identified in terms of a growth of awareness, specific regulatory or judicial rulings, and instances of success in limiting or preventing the use of information processing and surveillance technologies and systems that would otherwise have enjoyed free rein with our personal information. Meanwhile, academic discourse develops arguments about the relationship between law and technology, about the role of software 'code' in embedding rules in information systems, and about how individual property solutions can be brought to bear upon the situation.

This state of affairs is not a matter for complacency or cynicism. However, it provides

a context for looking at the latest tool that has come into view strongly since 2009: *accountability*. 'Accountability' – albeit, as Mark Bovens points out, a 'very elusive concept'[1] – is now a term in good currency among regulators, business, and consultants in the world of information privacy protection. They are developing practical accountability approaches, and critical debate is well underway. The roots of this accountability movement can be found in one of the oldest international instruments for data protection: the OECD Guidelines of 1981.[2] The 14th Guideline, the 'Accountability Principle', says: 'A data controller should be accountable for complying with measures which give effect to the principles stated above.' Those preceding principles are now the familiar ones concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, and individual participation in terms of individual rights to access one's own data and to challenge data with a view to having it erased, rectified, completed or amended.

There is further discussion of accountability in the 62nd explanatory paragraph of the OECD Guidelines document. It says:

> The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

It is clear that the term is used more or less to mean *responsibility* and *liability*, and it is likely that this is what data controllers, regulators and policy-makers have in mind

---

[1] Bovens, M., 'Analysing and Assessing Accountability: A Conceptual Framework', *European Law Journal*, 13, 4, 2007, pp. 447-68, at p. 448.

[2] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981.

when discourse and practice turns to 'accountability'. The Article 29 Working Party's understanding of terminology starts by being sensitive to these distinctions, only to give up the attempt at refinement in its closing sentences on terminology, as we see in its 2010 Opinion on the Principle of Accountability:

> 21. The term 'accountability' comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning – even though defining what exactly 'accountability' means in practice is complex. In general terms though its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.
>
> 22. In most other European languages, due mainly to differences in the legal systems, the term 'accountability' cannot easily be translated. As a consequence, the risk of varying interpretation of the term, and thereby lack of harmonisation, is substantial. Other words that have been suggested to capture the meaning of accountability, are 'reinforced responsibility', 'assurance', 'reliability', 'trustworthiness' and in French 'obligation de rendre des comptes' etc. One may also suggest that accountability refers to the 'implementation of data protection principles'.
>
> 23. In this document, therefore we focus on the measures which should be taken or provided to ensure compliance in the data protection field. References to accountability should therefore be understood as the meaning used in this Opinion, …[3]

An example of the elision of accountability with responsibility is found in the Treasury Board of Canada Secretariat's document of 2002, explaining its Privacy Impact Assessment (PIA) Policy, which requires privacy impact assessments to be performed by government institutions 'to evaluate whether program and service delivery initiatives involving the collection, use or disclosure of personal information comply with privacy requirements and to resolve privacy issues that may be of potential public concern.'[4] In a section entitled 'Accountability', the policy document states that senior officials in public organisations and others are 'responsible for' carrying out and ensuring the implementation of the PIA

[3] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, 13 July 2010. WP 173, paras. 21-3. The Working Party was established under the Data Protection Directive 95/46/EC.

[4] Government of Canada, Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy*, section on accountability, 2 May 2002.

policy through the performance of specific activities: in other words, what they must *do*. The 'Accountability' section does not, however, indicate what they must *say* about what they do, or say to whom, when, or how, although summaries of the PIAs themselves must be available to the public. We are therefore able to understand who is supposed to do what – a form of job description, possibly useful in bringing sanctions or rewards to bear, depending on the quality of the performance. But this approach is insufficient.

Concepts and Approaches

It would not be appropriate or possible to explore the large academic literature, both conceptual and empirical, on accountability in many fields of application: public administration, finance and accountancy, and professional fields such as education. Much of it concerns the elusive meaning of 'accountability' as a distinctive concept, and how it is used by practitioners as well as in academic discourse. Richard Mulgan has usefully traced these meanings, distinguishing between the *internal* and the *external* aspects of accountability, and highlighting as well as criticising the accumulation of further meanings.[5]

In brief, Mulgan argues that in the governmental world, internal accountability or responsibility has to do with the professionalism and personal morality or conscience of public servants and others in the exercise of their functions, and especially of their discretion. But within an organisation, it also involves accountability to hierarchical superiors, and therefore there is, in a sense, an element of externality as far as the individual official is concerned. On the other hand, external accountability for an individual or an organization involves some external agent or body in the assessment and investigation of actions or failures to act, and the imposition of sanctions. But these processes will also touch on professional and personal factors that explain the action; so the internal and external aspects are connected in complex ways. Nevertheless, Mulgan argues that 'a sufficiently robust distinction can still be

[5] Mulgan, R., '"Accountability": An Ever-Expanding Concept?', *Public Administration*, 78, 3, 2000, pp. 555-73.

maintained between having to account to someone else for one's actions and not having to do so.'[6]

Colin Bennett has also pointed out that accountability means more than responsibility.[7] Drawing on Mulgan, he points out that '[a]ccountability implies a process of transparent interaction, in which [an external] body seeks answers and possible rectification.'[8] In the context of data protection accountability, he also asks a crucial question: 'accountability for what and to whom?'.[9] It is especially the external form of accountability that we may want to use in the case of privacy protection, because it seems to correspond more closely to the relationship of data controllers to data subjects, as well as to regulators and the general public. Moreover, it involves the procedures and materials that are used in accountability, and in particular, the 'account' that is given externally, as we will see later.

There are unused dimensions in the concept of accountability that need to be examined and developed in the field of privacy protection. One of them is emphasised in another perspective that can be brought to the understanding of accountability: the idea of *stewardship*, by which is meant that one party entrusts another with resources and/or responsibilities.[10] Andrew Gray and William Jenkins argue as follows:

> To be accountable is to be liable to present an account of, and answer for, the execution of responsibilities to those entrusting those responsibilities. Thus accountability is intrinsically linked to *stewardship*. Stewardship involves two manifest parties: a steward or accountor, that is, the party to whom the stewardship or responsibility is given and who is obliged to present an account of its execution, and the principal or accountee, that is, the party entrusting the responsibility to the steward and to whom the account is presented. There is however, a third party in this relationship: the codes on the basis of which the relationship is struck and by which it is maintained and adjudicated. Codes may be explicit or more often implicit.[11]

---

[6] Ibid., p. 562.
[7] Bennett, C., 'International privacy standards: Can accountability ever be adequate?', *Privacy Laws & Business International Newsletter*, Issue 106, August 2010, pp. 21-3, at p. 21.
[8] Ibid.
[9] Ibid., p. 22.
[10] Gray, A. and Jenkins, W., *Administrative Politics in British Government*, Brighton: Wheatsheaf Books, 1985, p. 138.
[11] Ibid.; emphasis in original.

This idea enables us to relate the data protection case to the more general sense of political accountability in a democracy, in which there is a hierarchical relationship between superiors – the public – and the 'servants' who work for them as politicians and administrators. In data protection, data controllers are the stewards of the personal data they process, perhaps all the more because in many cases it was not specifically entrusted to them by the individuals concerned, but was received through other processes that, as we know, make data protection and compliance very difficult. Accountability, in the sense of acquitting the responsibilities of stewardship through the giving of an account, is therefore somewhat similar to another meaning of accountability as 'dialogue', in which 'officials…answer, explain and justify, while those holding them to account engage in questioning, assessing and criticizing'.[12] Although Mulgan has reservations about equating accountability with deliberative democracy among equals, the interactive dialogue between stewards and their principals, and the shared frameworks for explanation and justification that are negotiated between the two, make the 'dialogue' perspective an appropriate one for considering accountability, as a number of writers do,[13] and relevant in the case of privacy protection.

Gray and Jenkins go on to explain an elaborate typology of codes that are involved in the accountability relationship, according to several dimensions, although these cannot be enumerated here. However, an accountability code is:

> a system of signals, meanings and customs which binds the parties in a stewardship relation and governs the liability of the steward to present an account of the conduct of his stewardship. …it defines the nature of the relationship…, the content and manner of the execution of the specified responsibilities, and the terms in which the account of the execution is presented and evaluated.[14]

These authors also offer a dramaturgical perspective on the way accounts are presented, which adds important insights that could enrich our understanding of information privacy accountability. In theatrical as well as social interactions, actors on a stage and their audience may in some cases, and for various reasons, collude to

---

[12] Mulgan, op. cit, p. 569.
[13] The literature cited by Mulgan for this perspective is Day, P. and Klein, R., *Accountabilities: Five Public Services*, London: Tavistock, 1987; March, J. and Olsen, J., *Democratic Governance*, New York, NY: Free Press, 1995; Harmon, M., *Responsibility as Paradox*, Thousand Oaks: Sage, 1995.
[14] Gray and Jenkins, op. cit., p. 140.

sustain the performance, or the account, that is presented across the footlights or in everyday social encounters, as Erving Goffman analysed in terms of the 'presentation of self'.[15] Suspension of disbelief can also happen in political and governmental arenas when accounts are presented, according to Gray and Jenkins. This may involve subtle signals that the stewards need to improve their performance because the audience is unhappy, rather than the disputation between government and the public that may happen in political accountability where there is an implicit or explicit adversarial or quasi-judicial context for the giving and receiving of accounts.

It therefore seems important and timely to stand back and look further at the concept of accountability itself in terms of enhancing its practical meaning within the relationship among data controllers, other organisations, and the public. Such an examination involves looking at the root of the term, and considering what an 'account' is as an explanatory, communicative and evaluative performance that is separate from the activity it describes, and how accountability relates to transparency and trust. This understanding will help in assessing whether the current development of the principle and practice of data protection accountability satisfactorily embodies these meanings, or needs greater precision in order to become truly effective. The question, 'accountability to whom and for what?', is best answered if we have a clearer understanding of what an account is, and what its afterlife is, once it has been given to an external agent. The next section explores this.

The Nature of 'Accounts'

A parallel can be drawn between political accountability and social explanation, in the sense that, in a ideal world (but a world that one can hope to make real) they both share the same conditions of reasoned scepticism and agreement over the nature of the evidence that should be admitted to the discourse, and through which conclusions might be drawn.[16] To 'give an account' – *rendre des comptes* – is to tell a story, and

[15] Ibid., pp. 146-8. See Goffman, E., *The Presentation of Self in Everyday Life*, Garden City, NY: Doubleday Anchor Books.

[16] McPherson, A., Raab, C. and Raffe, D., 'Social Explanation and Political Accountability: Two Related Problems with a Single Solution', paper presented to the Symposium on Accountability at the Annual Conference of the British Educational Research Association, Leeds, September 1978, 34 pp.

there are three levels that can be distinguished. First, on a weak definition, it means the obligation of an organisation to report back, to 'give an account of its actions'. Second, on a stronger definition, it means that, plus the implication that the audience can interrogate the account and produce other accounts 'on their own account'. Third, on the strongest definition, it means the previous two plus the implication that sanctions can be brought to bear where there is a general agreement that the organisation has 'given a bad account of itself', either (a) through its inactions, or (b) through its own unsatisfactory production of an account. The audience, which may be the public, can thus 'hold the organisation to account', and that might have real consequences.[17]

Actions – for example, compliance with data protection rules – must be considered part of an account, because we may perhaps experience them and therefore can – perhaps incorrectly – infer something about the organisation's motives, policies or procedures, although there is always the question of whether our experience reflects intended or unintended consequences. But the account must also, and essentially, include descriptions and explanations of the actions, for two reasons. First, so that we can better understand the organisation's intentions and its understanding, or theory, of its own situation or how it might act in it. Second, because most of a steward's actions are invisible to the principal, and therefore have to be *re-presented*, through stories or accounts, explanations and justifications.

Let us consider an example. When a business firm presents its accounts to shareholders in an annual report, it is telling a story – in words, pictures, and other symbols – of its performance over the last year: what it made or sold, how it organised itself, how much profit or loss it made, whether it fulfilled its hiring policy, why it relocated a factory, and so on. It explains its successes and failures, its goals and targets, and its strategy. The financial part of the account is independently audited and found to comply with certain kinds of accounting standards and conventions. That those standards are socially constructed and shaped over time, rather than unalterably

---

roneoed; in the possession of the author. The present article quotes from and draws upon that paper, with the permission of Andrew McPherson and David Raffe. That paper, in turn, contributed to Gray, J., McPherson, A. and Raffe, D., *Reconstructions of Secondary Education: Theory, Myth and Practice Since the War*, London: Routledge & Kegan Paul, 1983, Chapter 17, 'Politics, Education and the Reconstruction of Research'. This was written jointly with the author, and is also drawn upon here.

[17] See the similar analysis in Bovens, op.cit.

'objective', is another question. But note that the manufacturing and the hiring and the planning and the selling are activities that are *separate* from the account that is given, the story that is told about them. The story may be embellished and sanitised, and the financial conventions might not tell the only story that could be told about the money, although they have been independently scrutinised and approved. The whole account constitutes *information* for its audience – the shareholders, the stockbrokers, the industry regulators, the general public – but it may also have an element of *propaganda* – a 'tall story' that is designed to encourage or maintain the confidence of investors and keep the share price buoyant. The glossy pictures of the boardroom executives tell a sub-textual story that is also designed to keep us happy – the right mix of genders and ethnic groups; all clean-cut corporate types with MBAs and possibly good military-service or public-service records as well.

Thus, the account is produced. It is also received by its audience. What happens next, and what ought to happen in fulfillment of the requirements of external accountability, are not often explored in conceptual terms, and seem completely lacking in the data protection discourse on accountability. The audiences for a company's account, who can bring sanctions to bear, might not be able directly to experience much of what the company has done in the past year, and therefore need to have the account. But how do they distinguish between information and propaganda? How do they test the account for truthfulness? The finances are vouched for by the auditors, but what about the rest of the account? Can it be challenged as a story? Can other, and different, stories be told using the same information but analysed and reported in different ways? Can other information be brought to bear upon it: information that has somehow been 'left out of account' or underplayed, such as a damaging labour dispute, a boardroom conflict that let the company drift for three months, a failure to gain valuable contracts owing to poor procurement tenders, the unemployment created in one place when the factory was moved elsewhere, or the resignation of a number of female Asian employees who were passed over for promotion? And do we, perhaps correctly, think the worse of the company because of these actions, even though they assure us that they do not reflect company policy, intentions, or ethos? Do we also think the worse of the company because these other stories were left out of the account it chose to tell?

So it is also with democratic politics, and the images, words and symbols that politicians and governments present to the electorate in accounting for their performance since the last election. The importance of having unimpeachable and transparent sources of statistical information about the economy, for example, is so that everyone can try to come up with alternative stories about the economy based on the same evidence; the incumbent politician's story about how growth is happening, unemployment shrinking, debt levels and inflation falling, and the like do not have to be taken at face value or as truth for no other reason than that it is impossible to tell any other story. Part of this will involve agreed meanings of key terms: unemployment, growth, debt or inflation, for example, and how these conventions are arrived at or negotiated, are also part of the accountability story.

What the audience can do in testing the account, or in challenging the story to see if it is correct – if it does not misrepresent the company's or the government's performance – may depend on a host of conditions that may or may not be fulfilled. Part of the possibility of challenging an account and giving a different one also depends on the existence of a free press and other media capable of undermining an account-giver's monopoly of information and its interpretation. On the other hand, alternative sources of information may not be available; the necessary skills of analysis may be lacking; or it might just be too boring. Or perhaps the audience who receives the account is only granted access to the 'results' shown in the account – the 'bottom line' of the balance sheet, for example, without being able to interrogate the raw data from which the account has been produced. Thus the question of transparency is crucial, but also the question of what counts as information in the accountability process. Furthermore, the audience must have the means to re-define the concepts and categories in terms of which the account is expressed, to propose alternative perspectives, and to back these up with evidence that might not be found in the organisation's own account; and, in turn, the audience must be able to defend its alternative through the same rules. In any case, what this suggests is that the audience for an organisation's or government's account must somehow be involved with the *process* by which the account is produced, and not only with the *product*.

But the point is already made: there is more to accountability than the production and receipt of an account as a proxy, in symbols, for the performance of the company in making things and in selling and so on – and in protecting personally identifiable

information. Much more can be said about the conditions for accountability in the sense being developed here: what the rules and procedures might be, whether they are rooted in data, how they might be are open to testing, how they might be amenable to the sceptical search for alternative explanations, and whether they invite dialogue with those who are not only an 'audience' but a constituency or a citizenry who are acted upon by the organisation or, indeed, a government or a data controller, and for whom the action that is reported in the account is consequential. There is no time to develop these parts of the argument, but the world of accountability in this organisational or political sense bears an uncanny resemblance to the epistemological procedures of scientific, or social scientific, practice and method through which theories are tested, including procedures for resolving disputes between accounts.[18]

Whichever mode of analysis we choose – whether emphasising dramaturgy, or the parry and thrust of alternative accounts and their arbitration towards an agreed result through the procedures of science or quasi-political disputation, or perhaps a combination of both of them – the short message is that 'accountability' is not a term to be trifled with, or used casually and rhetorically, or as a fashion accessory. It is a complex concept with deep implications for the relationship between organisations and the public, between stewards and those who invest them with responsibilities. It is a concept that is predicated on certain ways of knowing and certain kinds of knowledge, and on the empowerment of participants who require transparency as a condition of critical public discussion. These considerations establish a yardstick against which to measure the search for accountability in the protection of privacy.

Accountability for Information Privacy Protection

How well does the current accountability movement in information privacy protection stand up to these demanding conditions? How far does it enable the public to hold organisations to account for their stewardship of the personal information that they process? Is it a substitute for, or a complement of, other regulatory procedures? Colin Bennett has already given a brief answer, that the accountability movement in data

[18] Ibid.

protection is no substitute for judgments of adequacy, and that both are needed. Although some questions are answered by the developers of accountability approaches – for example, to whom is the data controller accountable, and what is she accountable (i.e., responsible) for? – this is not always the case, and organisations often give superficial assurances that only 'external and independent auditing' could verify. The audience needs more than just a recitation of company policy; as Bennett says, it needs to be able to get answers to:

> [a] deeper set of questions relat[ing] to internal mechanisms and procedures: 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?[19]

Bennett calls for the further development of third-party accountability mechanisms and verifiable instruments if accountability is to get off the page and into practice. This is probably necessary, and is in fact being pursued since 2009 as part of the Accountability Project, to be discussed below, but it still leaves somewhat unclear what the nature of the *account* should be, and how the external auditors and the like – 'accounting firms, standards bodies, seal and trustmark programs, [and] mediation and dispute resolution bodies[20] – should relate to the public whom they ultimately protect. Looking at the data protection accountability literature, little help can be found concerning these questions. Although, as Bennett points out, the 2009 Madrid Resolution's 'Accountability Principle' does say to whom an organisation must demonstrate its observance of principles and obligations (data subjects and supervisory authorities), the Resolution as a whole is couched in terms of what the 'responsible person' – 'any natural person or organization, public or private which, alone or jointly with others, decides on the processing' – is required to do.[21] It says nothing about what that 'demonstration' must consist of, how it is to be communicated, and what its dialogic afterlife might be in any forensic forum through which it could be debated. However, it does identify eight 'proactive measures' to promote better legal compliance, including organisations' privacy officers, employee

[19] Bennett, op. cit, p. 22.
[20] Ibid.
[21] *International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution*, Madrid: International Conference of Data Protection and Privacy Commissioners, 2009.

training, external and transparent audits, privacy impact assessments, and codes of practice.[22] Although this is not clear, presumably the adoption of such measures would form part of the organisation's 'demonstration', and feature in the account it gave.

It is true that the Resolution was only a sketch of what might subsequently be developed into a practical document. Further enlightenment comes from the Accountability Project pursued in Galway and Paris towards the development of privacy accountability that has taken place then and since, although there is still more to come from the Project. Here is how the Project construes 'accountability':

> [A]ccountability can be described as a *demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability. It encompasses expectations that organisations will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data.*[23]

The Project stipulated that an accountable organisation should 'demonstrate their accountable use and management of personal information',[24] and

> an accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to ensure responsible decision-making abut the management and protection of data.[25]

---

[22] Ibid., Article 22. These exemplary measures are commended in Article 29 Data Protection Working Party, op. cit., fn. 7.

[23] Hunton & Williams LLP, The Centre for Information Policy Leadership, 'Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project, October 2010' p. 2; emphasis in original.

[24] Hunton & Williams LLP, The Centre for Information Policy Leadership, 'Global Discussion on the Commonly-accepted Elements of Privacy Accountability – Galway, Ireland, April 29, 2009', p. 2.

[25] Hunton & Williams LLP, The Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements – a Document for Discussion, October 2009', p. 4.

The language of 'demonstration' is indeed everywhere: the word 'demonstrate' appears 19 times in 17 substantive pages in the Galway discussion document of October 2009, with no explanation of what a *demonstration* would entail apart from the actions or phenomena to which it is supposed to testify: the organisation's capacity and willingness to be accountable and to achieve privacy objectives; its possession of an infrastructure for responsibility; its commitment; its adoption of responsible policies; and the like. The demonstration will involve external, independent third parties and regulators, and internal monitoring. But it is hard to identify the material or conceptual culture of such demonstrations, apart from the very worthy materials and concepts regarding the organisation's *action* that the demonstration might re-present, or any clear indication that these elements of the communication and dialogue of accountability would need to be developed in successive iterations of the Accountability Project. Unlike our hypothetical company that buys and sells and then tells a story about that, the data-controlling organisation processes personal data, hopefully responsibly, but without conventional and routine ways of giving an account, or fixed times for giving it. To the contrary: the same document says:

> Accountability does not wait for a system failure; rather, it requires that organizations *be prepared to demonstrate upon request by the proper authorities* that it is securing and protecting data in accordance with the essential elements.[26]

Phase II of the Accountability Project migrated to Paris, producing a further document in October 2010. The comparative statistics are 30 mentions of 'demonstrate' in 10 substantive pages, but although there is little further enlightenment about the nature of accounts, the Project takes steps towards delineating an accountability regime for organisations that elaborates five 'essential elements' that have remained constant over the two phases. These elements are:

> (1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
> (2) Mechanisms to put privacy policies into effect, including tools, training and education.
> (3) Systems for internal, ongoing oversight and assurance reviews and external verification.

[26] Ibid., p. 10; emphasis added.

(4) Transparency and mechanisms for individual participation.
(5) Means for remediation and external enforcement.[27]

However, answers to Bennett's questions are somewhat clearer, as the Project has focused on the criteria for measuring or demonstrating accountability, in terms of the nine fundamental types of activity that an accountable organisation should undertake. These are:

(1) Policies
(2) Executive oversight
(3) Staffing and delegation
(4) Education and awareness
(5) Ongoing risk assessment and mitigation
(6) Program risk assessment oversight and validation
(7) Event management and complaint handling
(8) Internal enforcement
(9) Redress[28]

This description can be said to concentrate largely on the acceptance and infrastructure of *responsible behaviour*, and accountability is associated with the demonstration of these facts. This demonstration, as well as the measurement of achievement in terms of the nine items of activity, is to be done between the organisation and external agents who judge it. An alternative list, which is not exhaustive and not applicable to all organisations, was given by the Article 29 Working Party, which favours a general accountability principle to be built into the anticipated revised legislative framework for data protection in the European Union:

- Establishment of internal procedures *prior* to the creation of new personal data processing operations (internal review, assessment, etc);
- Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects.
- Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations,
- Appointment of a data protection officer and other individuals with responsibility for data protection;
- Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data

[27] 'Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project, October 2010', op. cit, p. 3.
[28] Ibid., p. 10.

(such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.

- Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects;
- Establishment of an internal complaints handling mechanism;
- Setting up internal procedures for the effective management and reporting of security breaches;
- Performance of privacy impact assessments in specific circumstances;
- Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc).[29]

More work would need to be done to develop the accountability codes and frames within which a company reported items on either of these lists, specifying the kinds of information needed by the external reviewers of these accounts. The closest the Project comes to this is with regard to its fifth 'fundamental', which concerns risk assessment and mitigation, particularly where Privacy Impact Assessment is involved: accountability would require transparency about the nature of the risk analysis, including the criteria used, how decisions are made to mitigate risk, and whether the steps taken are effective.

The Project envisages that third-party accountability agents and privacy supervisory authorities will play the crucial role in measuring the degree to which organisations fulfil their accountability in terms of the definitions, fundamentals, and essential elements adopted by the Project. The judgments of these external agents will be particularly important if an organisation wants to transfer personal data to foreign jurisdictions or to be relieved of certain regulatory administrative burdens. In these cases, certification may be a requirement; but short of that, validation procedures such as audits will be necessary. The Project has yet to clarify these validation and certification modes or procedures, and it will be important to see what emerges from its further deliberations. In relation to the question of accounts, the organisation will tell its stories to the third-party agent, and may even self-certify that it meets the requirements of accountability. This is far from what should be required if the concept of an 'account' were fully developed.

[29] Article 29 Data Protection Working Party, op. cit., para. 41.

As mentioned earlier, what the stories look like is critically important, but so too is the way in which they are questioned, challenged, verified or denied by the receiver of the account. In terms of the earlier argument, this can be understood in terms of both dramaturgy and scientific procedure, in moving towards accountability through openness and explicitness, scepticism, and the possibility of producing alternative accounts for arbitration through working towards agreement on what constitutes relevant and valid information, and how to resolve disputes. These are challenging requirements, and in the case of accountability for privacy protection they are shaped by the fact that the third-party agents and supervisory authorities have to stand proxy for the general public, who are the audience in the case of governmental or political accountability, given the specialised nature of this field. Therefore, in order to be satisfied that the accountability process for privacy protection is not undermined by the pressures and interests that are inevitable in this case, and by the desire – underlined by the Accountability Project – that the regulatory burden should be reduced, there should be further requirements. If not all of the nine 'fundamentals' are required in the accountability process for a particular organisation, to which the approach has been 'customized', then a further element of accountability will concern the basis upon which such customisation decisions have been made, the evidence introduced to support that argument for customisation, and the decision made by the external body to validate or certify that this selective application of the accountability requirements is proper, and could itself be open to challenge, scepticism, and alternatives. If the accountability *process* is to be trusted, it too must be transparent and open to these procedures, because the third-party agents and supervisory authorities are themselves stewards to whom the public entrust responsibilities, and accounts have to be given about that stewardship as well. In this situation, it could be argued that civil society organisations and others who are, in principle, congenitally independent, could play an important role. But they, too, would require to be accountable.

Conclusion

It is time to draw this discussion to a close. The question of accountability, and specifically for privacy protection, is highly complex, and focusing the spotlight on

the ‘account’ that lies at its heart adds to the complexity in one sense. But it also may provide some clarification of what needs to be established before one can either judge the adequacy of a proposed accountability procedure, or of the accounts themselves that become the informational and epistemological currency of the approach. It is important that these considerations be taken on board constructively in any development of accountability methods for the protection of information privacy.

References

Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, 13 July 2010. WP 173, Brussels: European Commission, 2010.

Bennett, C., ‘International privacy standards: Can accountability ever be adequate?’, *Privacy Laws & Business International Newsletter*, Issue 106, August 2010, pp. 21-3.

Bovens, M., ‘Analysing and Assessing Accountability: A Conceptual Framework’, *European Law Journal*, 13, 4, 2007, pp. 447-68.

Day, P. and Klein, R., *Accountabilities: Five Public Services*, London: Tavistock, 1987
Goffman, E., *The Presentation of Self in Everyday Life*, Garden City, NY: Doubleday Anchor Books, 1959.

Government of Canada, Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy*, 2 May 2002, Ottawa: Treasury Board of Canada Secretariat, 2002.

Gray, A. and Jenkins, W., *Administrative Politics in British Government*, Brighton: Wheatsheaf Books, 1985.

Gray, J., McPherson, A. and Raffe, D., *Reconstructions of Secondary Education: Theory, Myth and Practice Since the War*, London: Routledge & Kegan Paul, 1983.

Harmon, M., *Responsibility as Paradox*, Thousand Oaks: Sage, 1995.

International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution*, Madrid: International Conference of Data Protection and Privacy Commissioners, 2009.

March, J. and Olsen, J., *Democratic Governance*, New York, NY: Free Press, 1995.

McPherson, A., Raab, C. and Raffe, D., ‘Social Explanation and Political Accountability: Two Related Problems with a Single Solution’, paper presented to the Symposium on Accountability at the Annual Conference of the British Educational Research Association, Leeds, September 1978, 34 pp. roneoed; in the possession of the author.

Mulgan, R., ‘“Accountability”: An Ever-Expanding Concept?’, *Public Administration*, 78, 3, 2000, pp. 555-73.

Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981.

The Centre for Information Policy Leadership, ‘Data Protection Accountability: The Essential Elements – a Document for Discussion, October 2009’, Hunton & Williams LLP, 2009.

The Centre for Information Policy Leadership, 'Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project, October 2010', Hunton & Williams LLP, 2010.

The Centre for Information Policy Leadership, 'Global Discussion on the Commonly-accepted Elements of Privacy Accountability – Galway, Ireland, April 29, 2009', Hunton & Williams LLP, 2009.