A Cross-Disciplinary Review of the Concept of Accountability

A Survey of the Literature

Nick Papanikolaou, Siani Pearson

Security and Cloud Lab
Hewlett-Packard Laboratories
{nick.papanikolaou,siani.pearson}@hp.com

Abstract. In this paper we discuss previous definitions of the concept of *accountability* from the literature. Accountability is a multidimensional, context-dependent concept that is gaining interest as a means of addressing a number of data protection problems, including global legal uncertainty and lack of trust.

1 Introduction

Accountability is a complex, multidimensional concept that is subject to many different interpretations across a variety of disciplines. The concept is gaining currency in the context of data protection, and a number of regulatory frameworks are adopting accountability as an established term. This paper attempts to bring together a number of different definitions from a variety of sources, ranging from social and political science all the way to computer science. As will become evident from this short survey, there are commonalities and links between the different definitions and, while it is unlikely to find conflicting or contradictory interpretations, there are subtleties and distinctions in existing definitions that are worthy of our consideration.

2 Definitions of Accountability from the Literature

First we will consider high-level definitions and perspectives of accountability from social and political science, which will help us to frame accountability in the broadest possible sense.

Next we will turn to regulatory frameworks which make use of the term, and examine the relevance of accountability to the handling of personal data within organisations – particularly in the light of European laws and regulations related to data protection. Section 2.3 discusses accountability from the IT management perspective, and this leads us to section 2.4, which focuses down on computer science and presents

adfa, p. 1, 2011.

the interpretations of accountability used in that field, particularly in connection with the implementation of accountable systems.

2.1 High-level Definitions and Perspectives from Social Science

We consider a selection of definitions of accountability, starting with high-level conceptual definitions and proceeding toward a more organizational, governance-related view. We will look at conceptions of accountability from diverse disciplines.

Webster's dictionary of 1828 defines accountability thus:

"1. The state of being liable to answer for one's conduct; liability to give account, and to receive reward or punishment for actions. 2. Liability to the payment of money or of damages; responsibility for a trust."

This definition has changed in the latest version of the dictionary to exclude the reward and punishment aspects, which nevertheless are relevant to our present purpose. Key ingredients of this definition include attribution of responsibility ('being liable to answer for…'), giving explanations, receiving a penalty for any misconduct (especially, being financially liable for damages). These same ingredients are echoed in Schedler's definition (Schedler, 1999):

"A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, or justify them and to be punished in the case of misconduct."

Taking an organizational perspective, Koppell (2005) identifies five dimensions of accountability:

"1. Transparency: Did the organization reveal the facts of its performance?

2. Liability: Did the organization face consequences for its performance?

3. Controllability: Did the organization do what the principal desired?

4. Responsibility: Did the organization follow the rules?

5. Responsiveness: Did the organization fulfil the substantive expectation?"

Note that Koppell's definition identifies performance as the principal concern around which accountability is centred. Accountability is understood in relation to performance, which is the objective for which managers are held accountable. Jos and Tompkins (2004) explain that accountability processes can either be performance-based or compliance-based; most of the definitions of interest to us are geared towards compliance with prevailing laws and regulations.

The distinction between accountability and responsibility is made in the following definition (Galway, 2009): *"Accountability is the obligation and / or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions"*. The Galway project's definition of accountability refers specifically to the handling of personal data: *"Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."*

From the social sciences we have, among others, Romzek and Dubnick's typology (1987) of public sector accountability; this is a classification of the different ways in which public sector officials are held accountable, and emphasizes the responsibility and liability aspects of the concept of accountability. The typology distinguishes be-

tween legal, political, bureaucratic and professional accountability regimes, each representing a form of responsibility to a particular audience (e.g. bureaucratic accountability being defined as responsibility to those higher up in a bureaucratic hierarchy).

The privacy-oriented definition of accountability given in ISO standard 29100 (ISO, 2011) expresses accountability in terms of the practices associated with it in organizations:

"Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organization, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches."

This definition clearly picks out privacy breaches as being the problem that accountability as a whole is intended to address, and identifies specific ways to respond to the problem. It gives clear guidance on how to actualize accountability, avoiding what it is. Clearly it is desirable to combine some of the operational aspects with a high-level conceptual description of the concept, in order to produce a definition that meets the needs of researchers and practitioners alike.

Accountability concepts are evolving as the current legal framework responds to globalization and new technologies, and indeed the current drafts of the proposed EU Data Protection Regulation (EC, 2012) and US Consumer Bill of Rights (The White House, 2012) include this concept, at least at a conceptual level (see further discussions in Section 3.2 below). Region block compliance tools such as the EU's binding corporate rules (BCRs) (ICO, 2012) and APEC's cross border privacy rules (CBPRs) (APEC Data Privacy Sub-Group, 2011) are being developed to provide a cohesive and more practical approach to data protection across disparate regulatory systems (Moerel, 2011). See also 'The future of privacy', from the Article 29 Working Party (EC, 2009; Article 29 Working Party, 2012), its opinion of July 2010 (EC, 2010), and the Madrid resolution's global data protection standards (ICDPP, 2009), which the International Conference of Data Protection and Privacy Commissioners adopted in October 2009. The Galway/Paris project started by privacy regulators and privacy professionals has been defining the concept of accountability for the last four years in the context of these latest regulations (CIPL, 2009) and refining its implementation, measurement and scalability.

2.2 Regulatory Frameworks

Accountability is a tool being used by more and more regulators around the world, especially as privacy legislation is enacted or changed in response to technical change and globalization. It is increasingly popular in common law jurisdictions such as Australia, Canada and US and has gained more visibility and acceptance in places governed by civil law. It is not only in the legislation referred to above but also a concept included within enforcement powers in Canada and in new laws being introduced in Latin America (see for example, Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia, 2012).

Accountability as a notion established in guidance such as OECD (OECD, 1980), APEC (APEC Data Privacy Sub-Group, 2011) and PIPEDA (PIPEDA, 2000) essen-

tially means placing a legal responsibility upon an organization that collects and uses personal data to ensure that contracted partners to whom it supplies the personal data are compliant and equally accountable, wherever in the world they may be. Its notion as a data protection model is evolving towards being an 'end-to-end' personal data stewardship regime in which the enterprise that collects the data from the data subject is accountable for how the data is shared and used throughout its journey across the global and its lifecycle from collection to disposal.

The concept of accountability is enshrined in regulatory frameworks for data protection across the globe. The Organization for Economic Cooperation and Development privacy guidelines (OECD, 1980) do not only embrace the concept but also take a step forward, addressing it quite clearly by considering the data controller as accountable with regard to compliance with measures implementing the established principles. The concept of accountability is also present in the Asia Pacific Economic Cooperation's privacy framework (APEC, 2005), as well as in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, 2000). Basic elements of the concept can also be found in Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (Council of Europe, 1981). One expression of accountability that is common in all aforementioned documents are the obligations posed to the data controller for complying with that particular data protection legislation and, in most cases, the establishment of systems and processes which aim at ensuring such compliance.

Although the Data Protection Directive does not introduce explicitly the principle of accountability, it does embrace it in several provisions. The text of the Data Protection Directive as such is structured on the acceptance of relationships between the different entities involved in the processing of personal data. The relationship between data controllers and data subjects constitutes the main relationship provided on which further relationships are built. The Directive also addresses relationships from which accountability obligations derive between data controllers-data processors and data controllers-supervisory authorities. These relationships are characterized by a substantial imbalance of powers in practice in the course of processing between the data subject and the data controller, which justifies protection through accountability provisions (De Hert and Gutwirth, 2006). In his Glossary, the EDPS has defined accountability as follows: "accountability intends to ensure that data controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice (....)" (EDPS, 2012).

In January 2012 the European Commission presented a proposal for a draft Regulation that is suggested to replace the Data Protection Directive. Although the draft Regulation does not include the term accountability in its text, the Explanatory Memorandum explains that Article 22 of the draft Regulation, entitled 'Responsibility of the controller' "takes account of the debate on a 'principle of accountability' and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance".

The Article 29 Working Party in its opinion on accountability made use of the term 'accountability', but explained the reasons why it may be difficult to use the term in all European languages:

"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, without prejudice to finding another wording that more accurately reflects the concept given here. This is why the document doesn't focus on terms but pragmatically focuses on the measures that need to be taken rather than on the concept itself." (European DG of Justice, 2010)

The Article 29 Data Protection Working Party, national Data Protection Authorities (Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2010), the European Data Protection Supervisor (EDPS), as well as the data protection and privacy regulators at the 31st International Conference of Data Protection and Privacy Commissioners – see reference (ICDPP, 2009) - have paid special attention to the principle of accountability. The common ground of these approaches has been the need to "reinforce" (EDPS, 2012b) accountability implying clearly its existence under the Data Protection Directive. The Article 29 Data Protection Working Party has made use of the term "*reinforced responsibility*" in order to describe the meaning of accountability (European DG of Justice, 2010), implying both "responsibility" and "action" with respect to the specific responsibility. Both in the Opinion on the Future of Privacy (European DG of Justice, 2009) and in the Opinion on Accountability (European DG of Justice, 2010), the Article 29 Working Party examines primarily the "conformity in practice" of the processing conducted by data controllers with the applicable rules laid in the Directive. In this way, accountability seems to link the responsible actors with the implementation of certain measures.

2.3 IT Management

Governance and compliance frameworks such as ISO/IEC 27001/02 contain many of the elements of accountability defined above: the information security management system of an organization is meant to generate assurance, transparency and responsibility in support of control and trust. For instance controls within 27002 require attribution and separation of responsibility (e.g. ISO 27001 section A.8.1.1 states that "Security roles and responsibilities of employees, contractors and third party users

shall be defined and documented in accordance with the organization's information security policy."). Moreover, the increasing use of contractual arrangements and frameworks for monitoring the fulfilment of commitments made in those contracts affects liability (as breach of contract entitles the other party to some remedy at law. These remedies include payment of damages to compensate for the breach, termination of the contract, the ability to seek court orders requiring compliance, and a range of internal remedies such as reduction in charges, processes for negotiating consensual remediation without seeking court action, and so on).

Risk assessment is particularly important for accountability because it is a central part of the process used to determine and demonstrate that the policies (whether reflected in corporate privacy and security policies or in contractual obligations) that are signed up to and implemented by the organization (that is taking an accountability-based approach) are appropriate to the context. The type of procedures and mechanisms vary according to the risks represented by the processing and the nature of the data (CNIL, 2012; Catteddu, Hogben, 2009; Castelluccia et al., 2011). Automation can enhance this process (Pearson, 2011). Data impact assessment may also become an obligation for some high risk contexts within the forthcoming EU regulation (cf. Article 33: EC, 2012).

These elements of risk assessment, transparency and redress are captured within the core elements of implementing an accountability project within an organization specified within the Galway and Paris projects, which were (CIPL, 2009; CIPL, 2010):

- Policies that reflect current laws and relevant standards
- Executive oversight and responsibility for privacy
- Delegation of responsibility to trained resources; education of staff and suppliers
- On-going risk assessment and mitigation relating to new products or processes
- Regular risk assessment and validation of the accountability program
- Policies to manage major privacy events or complaints
- Processes to enforce policies internally
- A method of redress if privacy rights are breached

These core elements of implementing an accountability project within an organization (CIPL, 2010), are very similar to the guidance provided by the Privacy Commissioners of Canada, Alberta and British Columbia (Office of the Information and Privacy Commissioner of Alberta et al, 2012), which was influenced by that work.

2.4 Computer Science

Our interest is in bridging the gap between the high-level definitions and views of accountability that are found in legal, regulatory, and management texts, and those found in the computer science literature, in which there is to be found a stronger link to security controls and means of automating such aspects as assignment of blame, enforcement of policies and more.

The notion of accountability cuts across many domains of computer science, such as: digital forensics, computer security, distributed systems in general (including grid and cloud computing, the Internet and network applications) and natural language

processing. Except for a few references, esp. (Weitzner et al., 2008; Le Métayer, 2011; Pearson and Wainwright 2012), in computer science, there is not a general and interdisciplinary view of accountability. Most of the papers, due to the complexity of the concept, only address some properties or specific mechanisms related to accountability. One thing does become obvious though – namely the view that the preventive controls used extensively in classical IT security are not sufficient to achieve accountability. Full accountability requires mechanisms for information transparency, checking misbehaviour and responsibilities and then proceeding to punishment. There are already some proposals for frameworks integrating these aspects (Pearson and Wainwright, 2012) and formal models or logics for accountability (Cederquist et al., 2005; Le Métayer, 2009; Jagadeesan et al., 2009; Küsters et al., 2010; Feigenbaum et al., 2011).

Weitzner et al. (2008) consider that the usual "hide-it-or-lose-it" perspective on information is dominating but not adequate in a world where information should be communicated. They argue that a shift is needed from hiding information to ensuring only appropriate uses occur. They describe the ability to maintain a history of data manipulations and inferences (their interpretation of transparency) which can then be checked against a set of policies that govern them (their interpretation of accountability). For them, accountability is retrospective, in the sense that if actor *A* performs action *B* then we can review *B* against a predetermined policy to decide if *A* has done something wrong, and hence hold *A* accountable.

Lin (2010) claims that the key elements of accountability are: disclosure, liability and non-repudiation, and that the notion also includes collective responsibility and policy. Le Métayer (2011) discusses the interplay between legal and technical means to risks for citizens and consumers. Laws and contracts provide assurances and technology can help enforce legal commitments. Pearson and Wainwright (2012) take a global and interdisciplinary approach, which encompasses legal, regulatory and technical aspects. The principle is to provide a rich toolset rather than define a general, catch-all solution for all aspects of accountability. A distinction is made between *preventive*, *detective* and *corrective* mechanisms which can help in understanding, organizing and implementing accountability. Xiao (2012) is a comprehensive survey of research related to accountability in the computer science domain. The author does not give a precise definition for accountability but relates it to a number of uses in various areas of computer science. End-to-end accountability is generally not accomplished; these systems have four key characteristics: identities of events, a secure record of events, auditing and evidence.

3 Summary

In this paper we have reviewed existing definitions of accountability from the literature and discussed related concepts and their interrelationships; the way that accountability has been interpreted in regulatory frameworks has been reviewed in some depth, and various interpretations of the concept from different disciplines, from law to computer science, have been presented. Thus we have seen a great number of related perspectives and formal models of accountability that can be used in IT systems.

The ongoing Cloud Accountability Project (A4CLOUD), funded by the European Commission, has been working (among other things) on bringing these perspectives and models together to produce a coherent, cross-disciplinary view of this complex concept.

Acknowledgement. We would like to acknowledge the contributions of our colleagues in the A4Cloud project and, in particular, Jean-Claude Royer and Giles Hogben, to the analysis presented here.

4 References

1. Schedler, A. (1999). Self-Restraining State: Power and Accountability in New Democracies. Lynne Reiner Publishers, pp. 13–28.
2. Koppell, J. (2005) "Public administration review," *Public Administration Review*, vol. 65, pp. 94–108.
3. Jos, P. and Tompkins, M. "The Accountability Paradox in an Age of Reinvention: The Perennial Problem." Administration & Society 36 (2004): 255.
4. CIPL, Accountability Project (Galway Project): http://www.informationpolicycentre.com/accountability-based_privacy_governance/.
5. Center for Information Policy Leadership (CIPL) (2009) 'Data protection accountability: the essential elements. A document for discussion', available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (accessed on 1 March 2010).
6. Center for Information Policy Leadership (CIPL) (2010) 'Demonstrating and measuring accountability: a discussion document', Accountability Phase II – The Paris Project, available at http://www.huntonfiles.com/files/webupload/ CIPL_Accountability_Phase_II_Paris_Project.PDF (accessed on 2 July 2012).
7. Romzek, BS and Dubnick, MJ. (1987). "Accountability in the Public Sector: Lessons from the Challenger Tragedy." Public Administration Review. http://www.jstor.org/stable/10.2307/975901.
8. ISO/IEC 29100. (2011). Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27.
9. European Commission (EC) (2012) 'Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', January, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf (accessed on 2 July 2012).
10. White House (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
11. Information Commissioner's Office (ICO) (2012) Guidance on the Use of Cloud Computing, available at http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx
12. APEC Data Privacy Sub-Group (2011) 'Cross-border privacy enforcement arrangement', San Francisco, 18 September, available at http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf (accessed on 2 July 2012).

13. Moerel, L. (2011) ‘Binding corporate rules’, PhD thesis, Tilburg University.
14. European DG of Justice (2009). Article 29 Working Party. ‘The future of privacy: joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168)’, December.
15. European DG of Justice (2010). Article 29 Working Party. ‘Opinion 3/2010 on the principle of accountability (WP 173)’, July.
16. European DG of Justice (2012). Article 29 Working Party. Opinion 05/12 on Cloud Computing, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
17. ICDPP (2009). 31st International Conference of Data Protection and Privacy ‘Data protection authorities from over 50 countries approve the “Madrid Resolution” on international privacy standards’, available at http://www.gov.im/lib/docs/odps//madridresolutionpressreleasenov0.pdf (accessed on 2 July 2012).
18. Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia. (2012). Getting Accountability Right with a Privacy Management Program.
19. Office of the Privacy Commissioner of Canada (2007). "Privacy Impact Assessments." Internet: http://www.priv.gc.ca/fs-fi/02-05-d-33-e.cfm, February 2007 [Nov. 5, 2009].
20. Office of the Information and Privacy Commissioner for British Columbia (2012). Getting Accountability Right with a Privacy Management Program. Available at: http://www.oipc.bc.ca/guidance-documents/1435
21. OECD (1980) ‘Guidelines for the protection of personal data and transborder data flows’, available at http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (accessed on 2 July 2012).
22. APEC Data Privacy Sub-Group (2011) ‘Cross-border privacy enforcement arrangement’, San Francisco, 18 September, available at http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf (accessed on 2 July 2012).
23. PIPEDA (2000) Available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (accessed on 2 July 2012).
24. De Hert, P. and Gutwirth, S. (2006). ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’, in E. Claes, A. Duff and S. Gutwirth (eds.), Privacy and the Criminal Law, Antwerpen/Oxford, Intersentia.
25. EDPS (2012). Glossary of terms. http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability.
26. EDPS (2012b). Opinion on the Data Reform Package, 7th of March 2012.
27. EDPS (2012c). Opinion of the European Data Protection Supervisor on the Commission’s Communication on “Unleashing the potential of Cloud Computing in Europe”.
28. EDPS (2012d). “Responsibility in the Cloud should not be up in the air”. Article EDPS/12/15. Available at: http://europa.eu/rapid/press-release_EDPS-12-15_en.htm
29. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2010), ‘Ein modernes Datenschutzrecht für das 21. Jahrhundert’ (18 March 2010).
30. CNIL (2012) ‘Methodology for Privacy Risk Management’. Available at: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
31. Catteddu, D. & Hogben, G. (eds.) (2009) Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report, November.

32. Castelluccia, C., Druschel, P., Hübner, S., et al. (2011). Privacy, Accountability and Trust - Challenges and Opportunities, ENISA.
33. Pearson, S. (2011). Toward Accountability in the Cloud. Internet Computing, IEEE, July/August issue, 15:4, pp. 64-69.
34. European Commission (EC) (2012) 'Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', January, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf (accessed on 2 July 2012).
35. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.J. (2008). Information accountability. Communications of ACM 51(6), p. 87, June.
36. Le Métayer, D. (2011). Formal methods as a link between software code and legal rules. Software Engineering and Formal Methods , pages 3-18, http://www.springerlink.com/index/980H052715W527GQ.pdf.
37. Pearson, S. & Wainwright, N. (2012). An Interdisciplinary Approach to Accountability for Future Internet Service Provision. International Journal of Trust Management in Computing and Communications (IJTMCC), 1:1.
38. Cederquist J.G., Corin J.G., Dekker M.A.C., Etalle S., and Den Hartog, J.I., (2005). An audit logic for accountability. pages 34-43. IEEE, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1454301.
39. Le Métayer, D. (2009). A formal privacy management framework. Formal Aspects in Security and Trust , pages 1-15, http://www.springerlink.com/index/q7505648948p9710.pdf.
40. Jagadeesan R., Jeffrey A., Pitcher C., and Riely J. (2009). Towards a theory of accountability and audit. In Michael Backes and Peng Ning, editors, Computer Security ESORICS 2009 , volume 5789 of Lecture Notes in Computer Science , pages 152-167, http://dx.doi.org/10.1007/978-3-642-04444-1_10.
41. Küsters R., Truderung T., and Vogt A., (2010). Accountability: definition and relationship to verifiability. pages 526-535. ACM, http://dl.acm.org/citation.cfm?id=1866366.
42. Feigenbaum, J., Jaggard, A.D. and Wright, R.N. (2011) 'Towards a Formal Model of Accountability', In Sean Peisert, Richard Ford, Carrie Gates, and Cormac Herley, editors, NSPW , page 45-56. ACM, 2011, http://dl.acm.org/citation.cfm?id=2073276.
43. Lin K., Zou J., and Wang Y. (2010). Accountability computing for e-society. pages 34-41. IEEE, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5474671.
44. Xiao Z., Kathiresshan N. and Xiao Y., (2012). A survey of accountability in computer networks and distributed systems. Security and Communication Networks, http://dx.doi.org/10.1002/sec.574.
45. Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., and Postigo H. (eds.) (2012) Managing Privacy through Accountability. Palgrave Macmillan.
46. Raab C. (2012). The Meaning of 'Accountability' in the Information Privacy Context. In [45].
47. Bennett C. (2012). The Accountability Approach to Privacy and Data Protection : Assumptions and Caveats. In [45].
48. Alhadeff J., Van Alsenoy B. and Dumortier J. (2012). The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In [45].