Strong Accountability: Beyond Vague Promises

Denis Butin, Marcos Chicote, Daniel Le Métayer

Strong Accountability: Beyond Vague Promises[1]

Denis Butin, Marcos Chicote and Daniel Le Métayer

1. Introduction

Individuals share more and more personal data and are out of touch with what happens to their data after their release. The principle of *accountability*, which was introduced three decades ago in the OECD's guidelines (OECD 1980), has been enjoying growing popularity over the last few years as a solution to mitigate this loss of control by increasing transparency of data processing. For example, a consortium has been set up in 2009, with precisely the definition and analysis of accountability as one of its primary goals (CIPL 2009). At the European level, the Article 29 Working Group published an opinion dedicated to the matter two years ago (Article 29 Working Party 2010) and the principle is expected to be enshrined in the upcoming European data protection regulation (EC 2012).

The very popularity of the word yields suspicion. Its widespread use, combined with the lack of a unique definition, begs the question of whether accountability can be characterised precisely enough to achieve consensus and bring sufficient protection. Can one leave behind questions of terminology and elucidate accountability in a way congruent with most interpretations?

In addition, the concept of accountability has been mentioned in so many different settings that it is legitimate to wonder whether a precise and consensual definition, assuming it can be established, would be as broadly applicable as the larger interpretation of the concept seems to be. Is the notion of accountability so diluted that trying to pinpoint it would remove all the generality that caused its initial appeal as well as its expected virtues?

Finally, assuming accountability can be characterised precisely and is still a concept with broad applications, does it bear the capacity to deliver innovative solutions to long-standing problems such as loss of control over personal data? Could accountability turn out to be little more than an umbrella buzzword for a variety of old solutions merely rehashed under the guise of new terminology?

Even if all those concerns cannot be resolved easily, there is no reason to give accountability a blank check. Apprehensions over the possibility of an accountability strategy backfiring have been spelled out and need to be taken into consideration.

In this article, we will first review the reasons put forward to support accountability, as well as the criticisms raised against it (Section 2). It will become apparent how current and upcoming regulations are unsatisfactory in their way to address accountability when compared with requirements seen as essential by many sources.

Discussing accountability critically requires distinguishing between its application levels. We will emphasise what has sometimes been termed *accountability of practice*, the requirement that data controllers should be able to provide a statement (an account) showing that their actual data handling practice complies with their obligations. We contend that the resulting opacity of actual practices and excessive focus on procedures is harmful enough to derail the overall accountability approach. To overcome these limitations, we put forward *strong accountability*, which relies on precise legal requirements supported by effective tools (Section 3). We then show that such tools can be provided considering the state of the art in terms of technology and suggest an approach for *accountability by design* (Section 4). Of course, technical feasibility is

1 This work has been partially funded by the European FI-WARE project / FP7-2012-ICT-FI. See http://www.fi-ware.eu/

only a prerequisite, not a sufficient condition for effective adoption. As expressed by Colin Bennett (Bennett 2012), "there is little evidence that market pressures alone will push this kind of external conformity assessment". To address this issue, we also provide suggestions for an overall architecture for strong accountability, including legal and economic dimensions (Section 5). Finally, we put strong accountability in perspective and discuss its complementary with other privacy instruments such as Binding Corporate Rules, Privacy Impact Assessments, privacy by design and privacy seals (Section 6).

2. The Meanings of Accountability and the Question of its Value

While accountability is no new idea, its use in the field of privacy and data protection has increased considerably lately. To set up the stage, we sketch in this section some reference documents on accountability in normative documents (Subsection 2.1), in the legal doctrine (Subsection 2.2) and in the computer science literature (Subsection 2.3). Let us note that the goal of this section is not to present a comprehensive survey of accountability[2], but to provide some background information before discussing the pros and cons of accountability in Section 3.

2.1. Accountability in Regulation and Guidelines

In this subsection, we start with a quick review of some landmarks in terms of accountability before discussing their reception in the legal doctrine in Subsection 2.2 and the computer science view in Subsection 2.3.

2.1.1. The United States' FTC FIPPs

Accountability in the context of data protection is currently not enshrined in US law. This is not entirely surprising given the general orientation of US data protection law, which tends to favour self-regulation and only reluctantly impose binding commitments. As far as soft law is concerned, the US Federal Trade Commission's Fair Information Practice Principles (FIPPs) (US Federal Trade Commission 1973), a set of non-binding[3] guidelines that have been used as a basis for specific, sectoral laws such as the Right to Financial Privacy Act (Title 12 of the U.S. Code 1978), do not list accountability in their principles even though they refer to related concepts[4].

2.1.2. The 1980 OECD Guidelines

The introduction of accountability as a *basic principle* in the 1980 Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD 1980) is often cited as its first notable appearance. The precise wording of the Guidelines is the following: "A data controller should be accountable for complying with measures which give effect to the principles stated above". While the aim of these Guidelines is the effective protection of individuals' privacy, the additional goal of economic benefits through simplified data export procedures is evidenced by the second part of their title. As far as enforcement is concerned, one should note that the OECD cannot legislate but only issue *soft law* in the incarnation of guidelines or recommendations.

The *Detailed Comments* part of the Guidelines provides some details about accountability, even though the word itself is never defined. It is written that "Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance". An interesting precision is that accountability is still required from a data controller when it uses the services of a third party for data processing. However, the nature of the evidence and the entity receiving that account are not discussed. Some authors (Raab 2012) conclude that the sense in which accountability is used here is close to liability.

2 We refer the reader to Charles Raab (Raab 2012), Colin Bennett (Bennett 2012) and Daniel Guagnin et al. (Guagnin 2012) for a more complete review.

3 Note however that the FIPPs have been used as a basis for the US Privacy Act of 1974.

4 The fifth principle, *Enforcement/Redress*, states that " (…) the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them".

In 2011, the OECD published a report (OECD 2011) reviewing the principles of its original Guidelines, including accountability, in light of the new technological and regulatory landscapes. The rising role of the accountability principle is highlighted[5] and "reporting, audits, education, and performance appraisals" are mentioned as some of its components. However, the paragraph of the report[6] dedicated explicitly to accountability mainly addresses data export issues.

2.1.3. The Canadian PIPEDA

In terms of regulation, the 2000 Canadian federal[7] Personal Information Protection and Electronic Documents Act (PIPEDA) (Parliament of Canada 2000) also includes a principle of accountability. The stated intent of the act is to balance the protection of personal information with the support of electronic commerce. It is partly based on the Canadian Standards Association's Model Code for the Protection of Personal Information (CSA 1996) and was also heavily influenced by the aforementioned OECD Guidelines.

Of the ten *privacy principles* it includes, accountability is the first one. The principle states that "An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles". The concrete measure of designating employees responsible for ensuring company-wide accountability is therefore central to PIPEDA's interpretation of the notion. The fact that this privacy principle refers to all other principles enumerated in the act gives it an overarching, prominent tone.

Another important aspect is the responsibility of organisations for data transferred to third parties: the same section of the act states that an organisation's responsibility includes "(...) information that has been transferred to a third party for processing".

PIPEDA also addresses the issue of practical compliance to some extent, even though its specifications in this respect remain broad: "Organizations shall implement policies and practices to give effect to the principles". The need to provide for means of redress is also mentioned. While not all facets of accountability are made explicit in the Canadian act, it globally remains comparatively precise in its integration of the principle. For instance, it was innovative in shifting the focus of accountability "from the legal regime to the actual protections afforded by the receiving organisation." (Bennett 2012).

2.1.4 The 2004 APEC Privacy Framework and the Data Privacy Pathfinder Program

The Asia-Pacific Economic Cooperation (APEC) forum, an international organisation of 21 countries[8], defined a Privacy Framework (APEC 2004) that includes accountability as one of its 9 *information privacy principles*. Its first mention states that "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above". The document does not specify who should receive the evidence making accountability possible, and is not more explicit than the OECD Guidelines in terms of an actual definition of the concept.

Recently, the APEC started reconsidering the question of accountability in more detail in the scope of its Data Privacy Pathfinder (APEC 2009); in APEC terminology, a Pathfinder is a *cooperative project among participating APEC Economies*. This effort is mostly about facilitating regulated data exports. One of its prominent features is the *Cross-Border Privacy Rules* system, under which organisations, on a voluntary basis, can follow a set of rules with the goal of increasing the trust of consumers and partner organisations in their commitment to privacy. Applications are assessed by APEC-

5 Notably the fact that PIPEDA "used the OECD Guidelines as a starting point" while "moving the Accountability Principle to the beginning".

6 *Role of accountability*, p. 52.

7 In addition, provincial private sector privacy laws exist in Alberta, British Columbia and Quebec. The principle of accountability also appears in those provincial regulations, although in an implicit form.

8 Generally speaking, as pointed out by Colin Bennett (Bennett 2012), a number of countries engaging in APEC have no national data protection regulation, which makes the existence of this framework all the more important.

recognised *accountability agents*, "which may include trustmarks, seals, and other private bodies." (OECD 2011).

2.1.5. The Accountability Project

Launched by the Centre for Information Policy Leadership in 2009 and commonly termed simply *Accountability Project*, the *Accountability-Based Privacy Governance Project* is an ongoing collaboration between industry actors, non-governmental organisations and government representatives aimed at defining and disseminating components of a standardised accountability strategy. White papers are being released, and the fifth phase of the project, in 2013, discusses the specific challenges of distributed environments such as mobile applications and cloud computing.

Accountability is made more precise in the publications of the project. Notably, it adds the dimension of what could be called the *accountee* or entity receiving the evidence. Unlike the OECD Guidelines and the APEC Privacy Framework, the Accountability Project addresses this point. For instance, the white paper resulting from the second phase of the project (*The Paris Project*) mentions "Organizations may be accountable to three entities: data subjects/individuals, regulators, and business partners." (CIPL 2010).

The necessity of the link between regulation and concrete measures is articulated in the Paris Project document: "Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data". Charles Raab (Raab 2012) notes the frequent use of the notion of *demonstration* in the publications of the Accountability Project, reinforcing the idea that accountability implies the readiness by data controllers to show and explain their actions, possibly upon request – a kind of information transparency. The Project, like other think-tanks and regulations surveyed so far, however falls short of going into the details of acceptable practical mechanisms for demonstrable data protection. In addition, even though the role of third-party accountability agents is recognised, data controllers seem to keep the central role, which may cast doubts about the impartiality of the whole process.

2.1.6. European Law and the Upcoming Regulation

In European data protection law, there is no explicit principle of accountability of data controllers until now, even though one may argue that the accountability obligation is implicitly present. In its *Opinion on the principle of accountability* (Article 29 Working Party 2010), the Article 29 Working Party has advocated the introduction of an accountability principle defined as "showing how responsibility is exercised and making this verifiable." The verifiability aspect of this definition is important: it implies an audit, which opens the possibility of finding that a data controller did not comply with its obligations. The draft of the new regulation released in 2012 by the European Commission (EC 2012) indeed includes an article about accountability[9], even though the word itself is not used in the article, and the provisions are rather vague. Article 20 states that "The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation." and "The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to [in earlier paragraphs]". The draft regulation envisions delegated acts to further specify appropriate measures.

2.2. Legal Doctrine

The legal doctrine discusses both the fundamental values underlying the accountability principle and its effectiveness for data protection. As far as principles are concerned, Paul De Hert (De Hert 2012) establishes a link between accountability for privacy and human rights law by pinpointing the duty for EU member states to require effective data protection measures from organisations. More generally, he associates the concept of accountability with external scrutiny – implying the need for a recipient of the account – and with account giving – the keeping of a record, and its transmission to an authority.

Other authors see accountability as a focusing lens with the potential to address a range of issues with an integrated

9 Article 20.

approach: it "can form the focus for dealing with issues of scale in regulation, privacy risk assessment, self-regulation (…) and foster an environment for the development of new technologies for managing privacy." (Guagnin et al. 2012).

Charles Raab subscribes to this idea that accountability is a multifaceted notion, stating that not all of its aspects have been exploited yet: "There are unused dimensions in the concept of accountability that need to be examined and developed" (Raab 2012). He furthermore quotes the interpretation of accountability as *stewardship*: the entrusting of "resources and/or responsibilities" from one party to another. The importance of transparent data sources, the *accounts*, which empower *audiences* to come to their own conclusions regarding the interpretation of data, which should not be left solely to data controllers, is also emphasised. Indeed, many actions tend to be invisible, or at least do not leave a trace in event histories. This combination of facts and descriptions justifies seeing accounts as *stories*, possibly carrying elements of propaganda or bias. He also contends that not only the final account but also the process of manufacturing it should be visible by the audience if full transparency is the ultimate goal.

Taking an operational approach, Colin Bennett clarifies the different levels of accountability by distinguishing three layers: *accountability of policy*, *of procedures*, and *of practice*. He emphasises that excessive focus is often placed on the first one, resulting in only superficial guarantees; and furthermore states that few organisations provide accountability at the practice level, and that this level requires external audit to be credible. The ultimate onus is on data protection authorities to specify a coordinated list of acceptable verification mechanisms. In addition, the incomplete description of actors and evidence in existing regulations and guidelines is pinpointed: for instance, the OECD guidelines do not mention who is expected to receive the evidence.

Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier support the need for an accountability of practice as defined by Colin Bennett and an explicit account as stated by Charles Raab by declaring that *common accountability measures* as defined by the Article 29 Working Party "are mainly articulated in the language of principles and concepts" and not linked to practical mechanisms (Alhadeff et al. 2011)[10].

Many points made in this section are discussed in greater detail in the recent volume (Guagnin et al. 2012) resulting from the European Privacy Awareness through Security Organisation Branding (PATS) project[11]. We can see from the above examples that accountability in legal doctrine is often considered as requiring a more concrete, practice-oriented aspect where the nature of the evidence is made explicit. As we will see now, research in computer science concentrates heavily on this practical facet.

2.3. Accountability in Computer Science

Accountability in computer science is generally associated with very specific properties. An example of formal property attached to accountability is *non-repudiation*: for example, in an analysis of a certified email protocol, Giampaolo Bella and Lawrence Paulson (Bella 2006) see accountability as a proof that a participant cannot deny that he has taken part in the protocol and performed certain actions. The proof of non-repudiation relies on the presence of specific messages in the network history of security protocols. A complementary concept in this work is *fairness*: it is not possible that one agent obtains what they seek while the other does not.

Jan Cederquist et al. (Cederquist 2005) introduce another concept of *agent accountability*: in a data usage control system, an audit authority in possession of evidence should be able to check the formal proofs that entities have to provide to justify themselves. The focus here is on establishing a kind of evidence that is unforgeable, thereby guaranteeing the detection of inappropriate data usage.

Jagadeesan et al. (Jagadeesan 2009) define accountability as a set of mechanisms based on "after-the-fact verification" by auditors for distributed systems. Mathematics-based methods are used to rigorously check properties of "accountability-based systems" where the interaction between entities, including auditors, is modelled and trade-offs between "potentially conflicting design parameters" are explored. As in (Schneider 2009), blame assignment based on evidence plays a central role in this framework. Integrity (the consistency of data) and authentication (the proof of an actor's identity) are integral to

10 They however emphasise that too strict regulations would be a burden and an unacceptable cost for budding companies.
11 See the project website: http://pats-project.eu/

the communication model. Together with non-repudiation (Bella 2006), these rather technical concepts are often seen as pillars of the concept of accountability in computer science literature.

On the practical side, (Haeberlen 2009) outlines the challenges and building blocks for accountable cloud computing. Accountability is seen as a desirable property both for customers of cloud services, who need to know whether something went wrong, and for cloud service providers, who can handle complaints and resolve disputes more easily. The building blocks of accountability are defined as *completeness*, *accuracy* and *verifiability*[12]. Technical solutions to enable these characteristics on cloud computing platforms have been devised by the authors.

2.4. Conclusion: Overgenerality versus Overprecision

The above discussion of the perceptions of accountability in normative texts on the one hand, and in computer science on the other, show that there is quite a shift of emphasis between the two views: normative texts mostly focus on what Colin Bennett calls *accountability of policy* and *accountability of procedures* (internal rules, existence of a data protection officer, corporate training, organizational issues, etc.) while computer scientists place more emphasis on very specific technical requirements for *accountability of practice*. To fill this gap and ensure that technical means can effectively contribute to the implementation of accountability in a broader perspective, more interdisciplinarity is needed: *we need to get together*, as pointed out in (Guagnin et al. 2012). In the following section, we discuss in more general terms the potential benefits and limitations of accountability for privacy protection before suggesting ways to move forward considering technical, legal and economic aspects in Sections 4 and 5.

3. Accountability for Privacy Protection: Promises and Pitfalls

In the previous section, we have reviewed the definitions of accountability in a somewhat neutral way, considering the differences in terms of scope, level of precision and interpretation in the definitions proposed by different communities and authors. The key issue that we want to address now is the potential impact of accountability rules on privacy protection. In Subsection 3.1 we will analyse the reasons to support the view that accountability should play a key role in future privacy protection regulations before discussing the potential pitfalls of accountability for privacy in Subsection 3.2. In Subsection 3.3, we will build on these arguments to argue that (1) accountability principles should indeed become a pillar for privacy protection but, (2) for accountability to be able to play this role, its must meet an absolute requirement of precision at all levels[13]; in default thereof, accountability might turn into a deceptive packaging and a way to further weaken privacy protection.

3.1. Accountability as a Key Privacy Enabler

One commonality among the definitions reviewed in Section 2, which is at the core of the accountability concept, is its introduction of a set of obligations bearing on controllers: in other words, accountability is complementary to the a priori controls provided by most *privacy enhancing technologies* which make it possible for subjects to limit their release of personal data (e.g. through selective disclosure or the restriction of the disclosure to anonymised or sanitised data). The first and foremost motivation for accountability in the context of privacy is the issue that, after the disclosure of their personal data, subjects are powerless – they have no choice but to trust controllers to handle their data appropriately. But subjects do generally not have any reason to trust data controllers blindly – one could even argue that subjects often have good reasons to distrust them because many companies have strong economic interests in the exploitation of personal data. The potential benefits of accountability appear exactly in such situations where an actor has a sufficient amount of trust in another actor to rely on him for a given action (e.g. to collect his personal data and use it for a given purpose), but is still not completely sure that his confidence is not misplaced. Accountability provides further means to check what happens on the side of the controller when the data has been released and therefore to move from *blind trust* to *proven trust* (De Hert 2012). Actually,

12 Those characteristics are defined as follows: completeness means that all agreement violations lead to reports and supporting evidence; accuracy signifies that no violation reports are created if nothing went wrong; and verifiability means that evidence is checkable independently.

13 Definitions of the roles of all stakeholders, their respective commitments, the accounts, the audit procedures, sanctions, etc.

considering the ever-growing collection and flow of personal data in our digital societies, a priori controls will be less and less effective for many reasons, and accountability will become more and more necessary to counterbalance this loss of ex ante control[14].

The reasons why a priori controls lose effectiveness are varied: first, more and more data is collected without the subject knowing it (through various logs, web cookies, surveillance systems, mobile phone applications leaking personal data to application providers or third parties, etc.). Even when the subject is aware of the data collection and asked to provide his consent, this consent has become a fictitious protection because he generally does not take the time to read the privacy notice provided by the controller[15], does not understand its implications[16], or gives his consent for lack of a real alternative (because he needs to get access to information or to a service). Even in situations where the consent of the subject could be considered free and well informed, the privacy notice on which it is based is by no means a proof of actual behaviour of the controller. A privacy notice is a declaration of a controller at a point in time, but the relation between what is announced and the actual mechanics of personal data processing is invisible. Strong discrepancies can be observed between privacy policies and actual practices, which can be due to different causes: the data controller may provide misleading policies from the start, the system may evolve without maintaining its original privacy protection, certain controls may rely on actions of the personnel of the controller or on subcontractors, the staff of the controller or his subcontractors may not be well aware or informed about privacy commitments, etc. In addition, the controller himself is not immune to privacy breaches from malicious (or curious) insiders or external attackers. As a result, data subjects have no clear knowledge of how much privacy they give up, do not know what actually happens to their data, and have no way of noticing whether the data controller breaches his obligations. As distributed systems such as mobile or cloud computing become ubiquitous, data subjects lose touch even more with what happens to their personal data.

Even though accountability should by no means be seen as an alternative to substantive data protection requirements (Bennett 2012) or an encouragement to weaken principles such as data minimality, it can help mitigating this loss of control, firstly by making actual behaviour visible and verifiable. Indeed, another common thread in the definitions of Section 2 is that accountability relies on the creation of accounts and their audits. Regardless of when and by whom these audits are conducted, their goal is to provide more transparency in data processing and therefore to increase the level of trust that the subject can place on the data controller. Another major benefit of accountability is that it can act as an incentive for data controllers to take privacy commitments more seriously and put appropriate measures in place, especially if audits are conducted in a truly independent way and possibly followed by sanctions in case of breach. As pointed out by Paul De Hert (De Hert 2012), “the qualitative dimension of accountability schemes may not be underrated”.

3.2. Objections against Accountability

Accountability is not a principle that receives unanimous support, though. The criticisms of accountability can be based on three types of arguments:

1. Objections from the legal point of view: some lawyers argue that accountability does not bring anything new to the existing notions and legal instruments; others claim that accountability could even accentuate the imbalance of powers between data controllers and data subjects by providing deceptive protections.

2. Reservations based on technical arguments: the very implementation of accountability measures might introduce further risks of personal data breaches.

14 As stated in the Article 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability (Article 29 Working Party 2010): “Firstly, we are witnessing a so-called ’data deluge’ effect, where the amount of personal data that exists, is processed and is further transferred continues to grow. Both technological developments, i.e. the growth of information and communication systems, and the increasing capability for individuals to use and interact with technologies favour this phenomenon. As more data is available and travels across the globe, the risks of data breaches also increase.”

15 In the survey Privacy Notices Research by the Privacy Leadership Initiative, only 3% of respondents declared to “carefully read” privacy notices “most of the time”.

16 The sheer length of this type of document and their convoluted language often prevents users from finding straightforward answers to simple questions such as a promise not to share personal data with third parties or, in case of share, the precise list of third parties which can receive the data.

3. Warnings based on economic arguments: accountability rules would impose unacceptable burdens on the industry.

Let us consider each of these categories of criticisms in turn.

The manifold nature of accountability, combined with currently vague definitions in legal instruments, may lead some data controllers to promote accountability in the hope of avoiding more constraining and comprehensive regulations. An example of such trends is described in a recent report (Ernst & Young 2012): "To avoid greater regulation, organizations in the retail and consumer products industries and GS1, a supply chain standards organization, are working with privacy commissioners to voluntarily set guidelines that address the privacy implications of using radio frequency identification (RFID) technology in their operations". In the worst case, accountability could be implemented by light organisational measures, for instance by just having in place a data protection officer, an awareness plan and some executive oversight. When audits are conducted by the companies themselves or business associations, the subject may also be concerned about their neutrality: after all, why should he be more confident in self-audits than in self-declarations of privacy policies? For these reasons, accountability has been criticised for offering companies a cheap "data protection favourable" reputation even if their actual practices and accountability rules actually offer limited guarantees, amounting to "privacy greenwashing" (Guagnin 2012). In the same vein, the 2009 white paper (CIPL 2009) from the Accountability Project also draws criticisms from certain lawyers (Bennett 2012), as it mentions that an accountability strategy allows companies to reach data protection goals in a way "that best serves their business models."

More generally, accountability is often associated with self-regulation, which is a controversial approach. The main benefits of self-regulation are its flexibility and its wider acceptance in the industry: because the rules can be tailored to a given business sector and controlled by the concerned actors, these actors are more likely to follow them. More generally, considering the difficulty to regulate the Internet in the international context, self-regulation is often presented as an adequate solution to face the "disintegration of traditional sovereignty paradigms" (Poullet 2001). However, the validity of self-regulation as a norm has to be assessed against traditional criteria such as the legitimacy of its authors, the conformity of its content with respect to other legal rules and its effectiveness, including the possibility of sanctions (Ibid.). In the context of accountability, one could argue that the second criterion should generally be satisfied (it is to be hoped that the accountability rules defined by e.g. an industrial sector would comply with applicable laws), but the first one is not really satisfied unless a data protection authority officially endorses the rules (or the rules are defined in collaboration with the authority, which could be seen as a form of co-regulation), nor does generally the last one. It should be clear that the lack of real consequences for data controller breaching the code or the lack of effective control would seriously weaken the assurance provided by self-regulated accountability schemes.

Another critical view of accountability relies on the idea that it is just a superfluous notion because it is already implicitly covered by existing instruments. For example, Colin Bennett (Bennett 2012) argues that there is an "unfortunate tendency" to believe that "new constructs for privacy" are needed. According to him, the essential principles of privacy do not need reformulating to allow for accountability: its key aspects can be integrated in existing frameworks. To support this view, one may argue that legal wording such as "Article 22 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." in the draft General Data Protection Regulation released by the European Commission in January 2012[17] does not add very much to existing obligations. Even more striking are the following comments in the Working Party 29 Opinion on the principle of accountability (Article 29 Working Party 2010): "One may also suggest that accountability refers to the implementation of data protection principles", and "The Article 29 Working Party wishes to highlight that most of the requirements set out in this new provision actually already exist, albeit less explicitly, under existing laws"[18].

From the technical point of view, tensions can also arise between accountability and privacy: the accounts which form the basis of the accountability procedure can themselves involve personal data; enforcing the implementation and storage of these accounts therefore introduces an additional risk for these data. This can be the case, for example, when the accounts take the form of execution logs. Obviously these logs should be subject to strong security measures but, as experience has shown too often, there is no absolute security protection. Data minimisation should therefore be encouraged: only information essential for compliance checking should be recorded in logs. Efficiency is one reason but the main one is to avoid further spreading of personal data. Another concern on the technical side is the authenticity of the accounts. Because

17 Section 3.4.4.1.

18 Even though this suggestion is not exactly the definition adopted by the Working Party 29 in the rest of the document.

they are, by definition, built and stored by (or under the control of) data controllers, how can the auditor and the subject be convinced that they provide a faithful representation of the actual data processing? The accounts could have been forged by the controller to cover up privacy breaches or they could have been tampered with by external actors. Again, technical means can be implemented to enhance the trustworthiness of the accounts (Bellare 1997, Schneier 1999), but they cannot provide an absolute guarantee, which might become a problem if the accounts are to be used as evidence in legal proceedings.

Needless to say, binding accountability rules are not necessarily welcome in the industry because they would introduce additional obligations and potential costs. As discussed above, this fear can actually turn into a support for a weak form of accountability (focusing on light organisational measures adopted on a voluntary basis). This economic argument should be taken seriously though, as it would be illusory to believe that strong accountability measures could be imposed in any country if they had to result into unacceptable burdens on the industry, especially at a time when personal data has become the "oil of the new economy". We investigate promising paths to address these issues in the following sections.

3.3. Beyond Vague Promises: Need for Precise Commitments

We believe that the criticisms discussed in the previous subsection deserve great attention. First, the fact that accountability could turn into deceptive promises providing erroneous expectations to data subjects is of great concern. Indeed, if this grim prediction became a reality it would undermine the very value that accountability is supposed to restore, namely trust. To analyse the reasons why an accountability system could be misleading and provide to the subjects a false sense of protection, let us consider the characterisation of accountability proposed by the Article 29 Data Protection Working Party (Article 29 Working Party 2010): "its emphasis is on showing how responsibility is exercised and making this verifiable". To achieve this objective, it is necessary to know precisely: (i) what the responsibilities are, (ii) what pieces of evidence will make the verification possible and (iii) who will be in charge of the verification and in what conditions. Each of the objections in Subsection 3.2 can be related to a failure in one of these steps:

(i) If the commitments of the data controller are not well defined (and properly understood by the data subject) the guarantees provided by the accountability mechanisms are illusory. These commitments should obviously include all applicable legal obligations, but also any industry standards and declarations made by the data controller in his privacy statements.

(ii) If the pieces of evidence are not sufficient to establish that the commitments have been fulfilled, the verification process will not be reliable. This may be the case in particular if the evidence is incomplete or if no guarantee is provided about its integrity and authenticity.

(iii) If the actor in charge of the verification is not trusted by the subject, the whole accountability process will suffer from the same distrust. This would obviously be the case if the audits were conducted by the data controllers themselves or by representatives of their business sector.

The solutions to avoid these failures in the accountability process necessarily blend legal, technical and economic ingredients: the commitments of the controller involve legal obligations; the definition and analysis of the accounts have to rely on technical means; and the roles of all the stakeholders in the process must be integrated within a viable ecosystem. But the keyword and true imperative for all these aspects of accountability is *precision*: any doubt or uncertainty in the process would cause mistrust and subvert the whole approach.

Precision can also be an answer to the second criticism discussed above, i.e. the fact that accountability is a superfluous notion because it is already covered by existing instruments. Indeed, one may agree that if accountability remains a vague obligation as stated in Article 22 of the Draft General Data Protection Regulation (EC 2012)[19], it does not add very much to

19 §1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. §2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). §3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external

existing measures. Except for the designation of a privacy officer in certain circumstances[20] and the reference to a Privacy Impact Assessment (PIA) which is required only when "processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes", one may wonder whether this article does not merely make explicit obligations that data controllers already have to meet in case of control by a supervisory authority. In addition, the verification by "independent internal or external auditors" is required only "if proportionate", which can hardly inspire confidence to data subjects. This article adds very little because it lacks precision: the only mandatory items in the records[21] do not include any information that would allow an auditor to check that the controller has processed the personal data in a way consistent with his obligations and declarations. In other words, the Draft General Data Protection Regulation introduces no more than a form of *accountability of procedures*, in Colin Bennett's classification. As a matter of fact, it is significant that Article 22 heavily relies on references to other articles of the draft, which reinforces this impression of redundancy.

As far as technical issues are concerned, solutions have been proposed in the computer science community to enhance the integrity and authenticity of execution logs. For example "forward integrity" (Bellare 1997) ensures that an attacker taking the control of a computer in which the logs are stored cannot tamper with existing logs (even though he would obviously be able to delete them or to fake future logs). Similarly, techniques have been proposed to authenticate the log entries and to set up a selective access to them, e.g. for external auditors. Again, these techniques can provide strong guarantees if the requirements and assumptions (types of attackers, level of trust between the stakeholders) are precisely defined.

In the remainder of this contribution, we make the point that accountability, to yield real added value for data subjects in terms of trust, should:

- be defined precisely, in all aspects, including the contents of the accounts and the rules to decide if an account is compliant;
- include *accountability of practice* (in Colin Bennett's terminology), i.e., apply not only to declared policies or procedures but also to the actual data processing;
- be supported by independent audits to avoid any risk of accommodating attitudes of the auditors and mistrust from the subjects.

In the following section, we show that this kind of *strong accountability* can be supported by appropriate tools and in Section 5, we make some suggestions on the overall accountability architecture, including organisational, legal and economic aspects.

4. Technical Solutions for Accountability of Practice

The first condition for the advent of *strong accountability* is that it can be supported by effective tools. In this section, we outline the key components of an accountability system (Subsection 4.1) and illustrate them with a practical application, which allows us to draw some recommendations for *accountability by design* (Subsection 4.2). We also discuss the

---

auditors.

20 Article 35 §1: The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise employing 250 persons or more; or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

21 Article 28. § 2 : The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3).

limitations of these solutions (Subsection 4.3).

4.1. Key Accountability Components

The first step of the accountability process should be a clear definition of the privacy policy that the controller has to comply with. *Privacy policy languages* are a technical solution for specifying privacy policies in a machine-readable format. By using a well-defined (formal) syntax, these languages are amenable to automated processing. A number of such languages have been around for some time, such as P3P (W3C 2006), EPAL (IBM 2003) or SIMPLE (Le Métayer 2009). Other languages, such as XACML (OASIS 2013) and UCON (Park et. al. 2002, Lazouski et. Al. 2010) can also be used to define privacy policies, even though they are more general purpose. A distinction is usually made between *data access* and *data usage* languages; the former makes it possible to set fine-grained permissions for the initial access to data, while the latter can also be used to specify what can happen to the data after it has been accessed. Common examples are the use of data for a specific purpose, its deletion, its anonymisation or its forwarding to a third party. Some languages, such as XACML, are restricted to data access control[22]; others, such as UCON and PPL[23], combine both aspects. In practice, privacy policy languages make it possible to translate the wishes of a data subject, the promises of a data controller and their common agreement about the use of the personal data into a format that can be processed automatically. Therefore, privacy policy languages are the first building block of accountability of practice: by formalising agreements about the authorised uses of the data, they help structure the evidence (accounts), which is at the core of the principle of accountability. From the privacy policy, it is possible to derive the information that must be present in the accounts to establish their compliance.

Accounts for accountability of practice can typically take the form of *log files.* A log is essentially a detailed history of the events of the system, often in the form of a chronological list. Such files can be generated automatically and in real time by the execution environment of the system. Assuming the mechanism generating them is tamper-proof (Schneier 1999, Waters et al. 2004), logs make up the core of the evidence against which accountability is to be assessed for data handling systems.

The next requirement of an accountability architecture is the possibility of conducting audits. The formal nature of privacy policy languages makes it possible to design tools to conduct automated and rigorous checks of the logs. Such a *log analyser* compares the actual sequence of data handling operations (events) represented in the log with the predefined agreement between the data controller and the data subject as included in a joint policy. After having processed the log, the tool outputs a conclusion about the compliance of the actual events with the initial agreement. If the implementation of the tool itself is transparent[24], this process provides real guarantees and confidence about the analysis of the accounts. If the log is deemed non-compliant, such a tool can automatically pinpoint which event (or absence of event) caused the breach.

4.2. Illustration with PPL

To illustrate the framework suggested in the previous subsection, we focus now on an example of a privacy policy language that includes both data access and data usage features: the PPL language[25].

4.2.1. Specifics of the PPL Language

The PPL engine includes a negotiation feature, which allows the data subject and the data controller to express their preferred policies separately before comparing them automatically to decide whether they are compatible. If it is the case, a

22 XACML deals with access control.

23 PPL (PrimeLife Policy Language), based on XACML for its access control aspect, also includes many usage control features. It was developed by SAP (Trabelsi et al. 2011) as part of PrimeLife, a 36 month long European project with the goal of investigating "...how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities".

24 For example if its source code is available or can be checked by an independent third party.

25 The a posteriori compliance checking approach is not tied to any particular privacy policy language, but we present the specific example of PPL to give a clearer idea of how the strategy can look like concretely.

joint agreement (strict enough to accommodate both parties) called *sticky policy* (Karjoth, Schunter and Waidner 2002)[26] is generated and attached to the data; in case of incompatibility, a report detailing the mismatch is generated, allowing each party to reassess his privacy policy or to abort the interaction if no compromise can be reached.

In PPL, two central features are available to express privacy policies: authorizations and obligations. They are used both to express policy preferences (for subjects and for controllers), and to define the resulting joint agreements (sticky policies). The PPL *authorizations* feature a notion of *purpose* formalised by keywords such as "marketing" or "identity checking". Data controllers specify in their policies for which purposes they intend to use the personal data they would collect; data subjects, on their side, specify explicitly the purposes they would approve. For the controller and subject policies to be compatible and generate a joint agreement, all purposes listed by the controller must be part of the subject's list. Authorizations also state whether *downstream usage*, i.e. the processing of the data by a third party, is allowed.

The core mechanism of PPL is the *obligations* concept. An obligation consists of a *trigger* and an *action.* Triggers are specific events or circumstances (e.g. data being used for a specific purpose, or forwarded to a third party). Actions are the events that are meant to take place once the trigger has fired, i.e. when the specific event or circumstance has taken place. For instance, a policy may mention that the phone number of a data subject should be deleted after it has been used for the purpose of identity checking. In this case, the deletion of data is the action event, and the trigger is the use of the number for identity checking. To prevent data controllers from claiming that they will fulfil an obligation in an indefinite future, triggers include a maximum delay. A number of trigger events are predefined in PPL[27] and new ones can be added. For action events, which specify what should happen if the associated trigger fires, the same flexibility applies. Default actions include the sending of a notification to the data subject, the deletion of personal data, and its anonymisation[28].

4.2.2. Compliance Checking and Log Design Guidelines

PPL logs include both trigger and action events. Trigger events can be seen as promises, arising from the sticky policy, to be fulfilled in subsequent events by the data controller. If the log is compliant, the trigger event will be followed, at some point, by the action event imposed by the corresponding obligation. Temporal parameters are taken into account to check whether the action event was performed before the agreed deadline. Because of this constraint, all PPL log entries are timestamped. Furthermore, trigger events must carry identification tags so they can be referenced from action events. Without this tag, ambiguities may arise and propagate to the global compliance checking.

It must be emphasised that the structure of the logs must be considered carefully to ensure that a privacy policy is accountable. First and foremost, all relevant data handling operations must be represented precisely enough to prevent any ambiguity; the decision of what to include in the logs thus requires careful consideration. In case of insufficient expressiveness, one log entry may refer to several data handling events, yielding different consequences on overall compliance. This precision requirement is complicated by the potential need for the data controller to minimise the amount of data stored in the logs for reason of efficiency or intellectual property protection.

The frequent subcontracting of data handling to third parties raises other issues: not only have the outsourced data handling operations also to be logged but sufficiently detailed information must be kept in the logs to settle disputes in case of malfunctions or breaches of obligations on the third-party side. Log architecture design and precise definitions of accountability are intertwined, and evolving circumstances can alter the distribution of responsibilities – these changes ought to be reflected in logging systems. Both the contents of the logs and their format are directly influenced by the way responsibilities are distributed among the main data controller and (possibly multiple) third parties.

Another source of complication may be the need to support *break-glass situations*[29], which refer to circumstances under

26 Sticky policies have also been used in the field of digital rights management; however, they play a very different role in our context because here they are checked a posteriori (rather than on the fly) and the process is audited by third parties.
27 Such as the use of personal data for a specific purpose, its forwarding to a third party, its access by the subject, etc.
28 Anonymisation is technically realized through cryptography.
29 Referring to the breaking of glass to trigger an alarm.

which exceptional access to data should be granted to an entity that does not possess the required privileges (NEMA/COCIR/JIRA 2004)[30]. This type of situation should be part of the scenarios supported by compliance checking mechanisms; hence the structure of logs must support them. Complementary human assistance may be required to prevent abuse of such mechanisms. Nevertheless contextual data ought to be included in the logs in conjunction with data handling events so as to accurately express the combination of modalities characterising break-glass situations.

The guidelines sketched in this subsection result from the experience gained while developing an accountability system for the PPL language. More detailed illustrations of these issues are described in (Butin, Chicote and Le Métayer 2013).

4.3. Challenges and Limitations of Technical Solutions

Since the technical framework outlined here is based on the analysis of logs, these logs must be truthful. More precisely, they ought to display the following properties:

1. It should not be possible for a DC to create fake logs: in other words, logs should reflect the actual execution of the system, especially in terms of personal data processing (*unforgeability*).
2. Once logs are generated, it should not be possible to alter them without detection (*integrity*).
3. It should be impossible to access logs without proper credentials (*confidentiality*).

Confidentiality can be achieved by encoding logs with cryptographic tools but care must be taken to allow for selective access: one cannot simply encrypt all logs at once, since different entities (e.g. auditors, subjects) should be granted access to different parts of the logs. The second property, integrity, can be supported by techniques such as the ones proposed by Bellare (Bellare 1997).

Unforgeability is the most challenging objective because it depends on the whole architecture of the system. Ideally, the architecture should be designed with accountability requirements in mind, so that verifying unforgeability can be made easier. This kind of architecture, for instance featuring a single decision point for all access requests to personal data, should make it easier to check informally whether logs reflect the actual events. The highest level of assurance would be attained through the application of mathematical modelling (*formal methods*). In this approach, all components playing a role in personal data processing and log generation must be accounted for. However, formal methods tend to be costly and could be applied only to the most critical parts of the system.

Great care should also be taken to minimize the ambiguities of log contents. Consider the example of ontologies in PPL: one of the available data handling events corresponds to the use of personal data for a specific purpose. A list of purposes can be agreed on, but simply defining a list seems insufficient: the ontology could be misused by stretching the meaning of words, claiming that the different available purposes where never clearly defined. This could be addressed by attaching informal statements of intent by the data controller to corresponding data handling events. Requiring data controllers to word their intentions in more detail should increase the pressure on them not to misbehave.

A different limitation is that some obligations defined by policy languages may not be checkable automatically, requiring human intervention. Integration of this aspect within an interactive verification tool is feasible but not straightforward; this kind of tool would produce hybrid compliance arguments involving both mechanical and manual steps.

Generally speaking, most of the necessary tools for the implementation of accountability already exist, but they must be used and combined carefully to yield a credible framework. Many challenges of this approach are therefore as much organisational as technical. On the other hand, no bullet-proof solution exists and the very purpose of accountability is to make it more difficult and more risky for data controllers to misbehave, not to enforce correct behaviours. In the next section, we take a closer look at non-technical challenges and solutions for an integrated accountability approach.

30 Common examples include the exceptional access to medical records in life-threatening situations, credit card fraud scenarios and military information classification systems (Feigenbaum et al. 2011).

5. Accountability Architecture: Legal and Economic aspects

In the previous section, we have shown that *strong accountability* is possible from a technical point of view and we have suggested practical means to support it. Obviously, it is not because strong accountability principles are technically feasible that they will actually be implemented. The next questions to address are therefore: should they be adopted on a voluntary basis (and why would this happen?) or should they be enforced by the law (and how)? What should the roles of the stakeholders (data controller, data subject, data protection authorities, third parties) be? What would be the costs and benefits for the industry?

First, following Colin Bennett (Bennett 2012)[31], it is unlikely that large-scale accountability can be adopted on a voluntary basis. Regulation should therefore impose binding accountability requirements. But such regulation should take into account two essential requirements:

- As argued in Subsection 3.3, just recalling general or vague accountability principles is not enough, and it could even provide a false sense of protection. Legal uncertainty would undermine the very principle of accountability.
- As stated by the Article 29 Working Party (Article 29 Working Party 2010), accountability should not impose "cumbersome new legal requirements upon data controllers, particularly given the current, challenging EU economic situation."

To solve this tension between the need for precise legal obligations on the one hand and economic acceptability on the other hand, we should stress that precision does not necessarily mean lack of flexibility. Indeed, it should be clear that a one-size-fits-all approach would not make sense in this area and different factors, such as the type of personal data at stake and the size and activities of the company, have to be taken into account to determine the required level of accountability and the associated measures. Also, because laws (and European regulations) should remain at a sufficient level of abstraction to be of general application and to avoid quick obsolescence, they should not go into the details of the accountability process but rather provide high level requirements imposing the necessary level of precision[32]. For example, following the recommendations of Section 4, they should state that any information or event which could have an impact on the data protection requirements must be recorded in the accounts, without defining what these events are and how they should be recorded. They should define the requirements for audits (periodicity, level of detail) depending on the situation. Such a flexible, multi-tier approach does not contradict the precision requirement: it should always be possible for the data subject to know, for a given controller, his privacy policy, the precise accountability measures implemented, the auditors, as well as the way to interact with them to be informed of the results of their audits.

This combination of legal requirements, flexibility and transparency is instrumental to restore the trust of the data subjects. It is also the key to economic viability of strong accountability: each data controller could decide to opt for the minimal requirements imposed by the law (both in terms of privacy policy and accountability measures) or to provide higher guarantees and use them as a business differentiator to get a competitive advantage.

As far as the extra costs incurred by the mandatory accountability requirements are concerned, they can be separated in three parts:

(i) Organisational costs: for staff training, privacy officer activities, documentation keeping, etc.

(ii) Technical costs: to build, store and secure the accounts.

(iii) Audit costs.

Category (i) should not represent significant additional costs, as it mostly corresponds to tasks already carried out by data controllers. Otherwise, they represent true sources of improvement of the quality of data handling procedures and overall

31 "Privacy audits have been around for a long time, but there is little evidence that market pressure alone will push this kind of external conformity assessment around the international economy".

32 "Technology neutrality has long been held up as a guiding principle for the proper regulation of technology, particularly the information and communications technologies" (Reed 2007).

internal organisation of the company[33].

Category (ii) can be reduced to marginal costs if accountability obligations are considered in the design of the system itself, following an *accountability by design* approach as suggested in Section 4.

As far as Category (ii) is concerned, the frequency of the audits and the associated costs should be proportionate to the level of sensitivity of the data and the size and type of activities of the controller. Technical tools such as the log analyser sketched in Section 4 can also help reducing audit costs.

In any case, as stated in Subsection 3.3, audits should be conducted by independent third parties: this is an essential condition for accountability to play its trust enhancing role. As mentioned by Colin Bennett (Bennett 2012), "the 'trust me, my account is the truth' approach will not be sufficient for many organizations". Furthermore, one may argue, following Paul De Hert (De Hert 2012), that external review is at the core of the concept of accountability: "It was brought into twentieth century public administration literature to denote the external scrutiny process, as opposed to the inner responsibility processes of the individual as per his or her conscience or moral value". Both high-level aspects of accountability such as company policies and practice-oriented aspects (through data handling log compliance checking) should be subject to audit.

But how should this independence be established and what kind of actor could play this role? We believe that in this matter inspiration could be taken from certification schemes, in particular information technology security schemes such as the Common Criteria for Information Technology Security Evaluation (Common Criteria 2013) in which national authorities can deliver accreditations to independent evaluators who are themselves in charge of conducting the evaluations. Similarly, data protection authorities, which do not have the resources to conduct large scale, country-wide audits could deliver accreditations to data protection auditors. A first step in this direction has been made in France with the introduction of the CNIL audit procedure seals in 2011 (CNIL 2011). The number of auditors approved by the CNIL is not very large yet but this business would obviously grow if strong accountability with independent audits became mandatory. Lobbying could prove to be a challenge in this area, and solutions such as anonymous auditing ought to be explored.

As far as efficiency is concerned, such an ecosystem of auditors could also help data protection authorities facing growing needs for controls, considering that their own resources cannot be extended ad infinitum. Of course, data protection authorities should keep the power to supervise on a regular basis the activities of the auditors themselves, to ensure that they keep a high evaluation standard, but auditors are necessarily much less numerous than data controllers. This monitoring of the whole process by data protection authorities would be essential, especially if the choice of the auditor is made by the data controller itself, which could otherwise lead to a quality dumping race among auditors.

Another benefit of accountability for data protection authorities is pointed out by the Article 29 Working Party: "putting the accountability principle into effect will provide useful information to data protection authorities to monitor compliance levels. Indeed, because data controllers will have to be able to demonstrate to the authorities whether and how they have implemented the measures, very relevant compliance related information would be available to authorities. They will then be able to use this information in the context of their enforcement actions."

Last but not least, for accountability to fully play its deterrence role, data protection authorities should have powers of sanction, not only to punish data controllers who have breached substantive data protection principles but also those who do not meet their accountability obligations. Penalties should be especially severe if the accounts provided by the data controller are proved to be inaccurate or forged, the same way organisations manipulating their financial accounts are severely sanctioned.

---

[33] To this respect, it would be advisable to introduce accountability as a new requirement of Information Security Management Systems (ISMS).

6. Accountability and Perspectives

In this paper, we have argued that *strong accountability* should be a cornerstone of future data protection regulations. By "strong accountability" we mean a principle of accountability which

- applies not only to policies and procedures, but also to practices, thus providing means to oversee the effective processing of the personal data, not only the promises of the data controller and its organisational measures to meet them;
- is supported by precise binding commitments enshrined in law;
- involves audits by independent entities.

As discussed in Section 5, we believe that this quest for precision is critical to ensure the effectiveness of accountability, and therefore of substantial data protection principles, and it should not be contradictory with the need for flexibility that is required by the industry. Generally speaking, a system where data controllers are audited by officially recognised third parties that are themselves accredited by data protection authorities would provide a consistent and efficient integrated accountability approach featuring a chain of trust all the way between supervisory authorities and data subjects.

Strong accountability should benefit all stakeholders: data subjects, data controllers, and even data protection authorities whose workload should be considerably streamlined. Indeed, if standardised accountability mechanisms become widespread, it would be far more efficient for data protection authorities to evaluate data controllers against well-defined criteria. Here, a form of standardisation would benefit both data protection authorities, which would enjoy a reduced workload, and data controllers, who would know in advance and more precisely to which metrics they must conform.

A further question could be the relationship between strong accountability and other instruments for privacy protection which have received a lot of attention during the last decade such as *Binding Corporate Rules* (BCRs), *Privacy impact assessments* (PIAs), *privacy by design* and *privacy seals.*

The European Commission defines BCRs as "internal rules (such as a code of conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection"[34]. The 1995 Directive's adequacy model, whereby permissions to export data depend on the country of destination, is ill-fitted to current data transfer practices. However, its derogation[35] permits transfers to countries deemed inadequate if "the controller adduces adequate safeguards". A working document by the Article 29 Working Party (Article 29 Working Party 2003) states that Binding Corporate Rules (BCR) can be considered as an acceptable safeguard to this respect. But BCRs have shown some limitations, in particular in terms of enforceability. As stated in (Alhadeff et al. 2011), "the integration of accountability mechanisms could be used to extend the existing adequacy regime. Our experience with Directive 95/46/EC has shown that the applicability of legislation offering 'adequate' safeguards does not by itself ensure that appropriate guarantees are implemented in practice". Indeed, it may be argued that the additional protection provided by accountability is even more necessary in case of international transfers of personal data.

PIAs (Wright 2011, Wright et. al. 2012) constitute a fundamental approach to evaluating risks: potential issues should be foreseen and analysed in a collaborative and interactive way before the design and deployment of a new system. As stated by Gary Marx, "It anticipates problems, seeking to prevent, rather than to put out fires". PIAs have thus to be conducted at the earliest stages, before a system is deployed. They should result into recommendations and requirements about the system and organisational measures. These recommendations should be taken as input to a privacy by design process resulting in an implementation of the system. This implementation can be evaluated by independent experts to get a privacy seal, which provides some guarantees about the fact that the system meets well-defined privacy requirements (including legal obligations) in terms of privacy. Strong accountability, in contrast with PIAs and privacy by design, concerns the

34 http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm
35 Article 26 (2).

practices, hence the effective exploitation of the product or system. In other words, it is an a posteriori rather than an a priori control. PIA do offer benefits, but as an ex ante analysis: they offer no guarantee regarding the actual processing of data.

However, as shown in Section 4, accountability does not emerge spontaneously. A system has to be designed with accountability requirements in mind, and these requirements should arise from the PIA. Indeed, the feasibility of accurate and comprehensive a posteriori verifications depends directly on the architecture of the technical platform under consideration. The privacy by design approach should thus include an *accountability by design* component, to ensure that accountability will indeed be feasible. This accountability component could also be evaluated as part of a privacy seal mechanism[36]. More generally, we should envisage in the long term a continuum between privacy seals and the regular audits required by strong accountability: the privacy seal would be the original certificate, providing well defined guarantees about the design of the system and the organisation in place, while accountability certificates would complement the original seal with guarantees about the effective use of the system. In this architecture, strong accountability could take the form of continuous maintenance of the original privacy seal. This maintenance could also have an impact on risk assessment (for example through the identification of new risks) leading to a new iteration of PIA and a virtuous improvement process.

References

Alhadeff, Joseph, Brendan Van Alsenoy and Jos Dumortier. "The accountability principle in data protection regulation: origin, development and future directions." Paper presented at Privacy and Accountability 2011, Berlin, Germany, April 5-6, 2011.

Article 29 Data Protection Working Party. *Opinion 3/2010 on the principle of accountability*. 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf. Accessed 28 February 2013.

Article 29 Data Protection Working Party. *Working Document on Transfers of personal data to third countries: Applying article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*. 2003. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf. Accessed 28 February 2013.

Asia-Pacific Economic Cooperation, Electronic Commerce Steering Group (ECSG). *APEC Privacy Framework*. 2004. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx. Accessed 28 February 2013.

—. APEC Data Privacy Pathfinder Projects Implementation Work Plan - Revised. 2009. http://aimp.apec.org/Documents/2009/ECSG/SEM1/09_ecsg_sem1_027.doc. Accessed 28 February 2013.

Bella, Giampaolo and Lawrence C. Paulson. "Accountability Protocols: Formalized and Verified." *ACM Transactions on Information and System Security 9 (2006):*138-161.

Bellare, Mihir and Bennet Yee. *Forward integrity for secure audit logs*. Technical Report CS98-580, Department of Computer Science and Engineering, University of California at San Diego, 1997.

Bennett, Colin. "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats." In *Managing Privacy Through Accountability*, edited by Daniel Guagnin et al., 33-48. Basingstoke: Palgrave Macmillan, 2012.

Butin, Denis, Marcos Chicote and Daniel Le Métayer. "Log Design for Accountability." Proceedings of the 4th International Workshop on Data Usage Management. Washington, D.C.: IEEE Computer Society, 2013.

Canadian Standards Association. *Model Code for the Protection of Personal Information (Q830-96)*. Mississauga: CSA, 1996.

Cavoukian, Ann. "Privacy by Design [Leading Edge]." *IEEE Technology and Society Magazine 31* (2012):18-19.

Cederquist, JG, Ricardo Corin, M.A.C. Dekker, Sandro Etalle and J.I. den Hartog. "An Audit Logic for Accountability." Proceedings of the 6th International Workshop on Policies for Distributed Systems and Networks. Washington, D.C.: IEEE Computer Society, 2005.

Centre for Information Policy Leadership. *Global Discussion on the Commonly-accepted Elements of Privacy Accountability*. 2009. http://www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Summary.pdf. Accessed 28 February 2013.

—. *Data Protection Accountability: The Essential Elements.* 2009. http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf. Accessed 28 February 2013.

—. *Demonstrating and Measuring Accountability: A Discussion Document*. 2010. http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF. Accessed 28 February 2013.

Commission Nationale Informatique et Libertés (CNIL), Label CNIL procédures d'audit de traitements. 2011.

36 See for example EuroPriSe, the European privacy seal: https://www.european-privacy-seal.eu.

http://www.cnil.fr/la-cnil/labels-cnil/procedures-daudit/. Accessed 28 February 2013.

Common Criteria for Information Technology Security Evaluation. http://www.commoncriteriaportal.org/cc/. Accessed 28 February 2013.

De Hert, Paul. "Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law." In *Managing Privacy Through Accountability*, edited by Daniel Guagnin et al., 193-232. Basingstoke: Palgrave Macmillan, 2012.

Ernst & Young. "Privacy Trends 2012. The case for growing accountability." 2012.

European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*. Brussels: European Commission, 2012.

European Parliament and the Council of the European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*. Brussels: European Parliament, 1995.

Feigenbaum Joan, James Hendler, Aaron Jaggard, Daniel Weitzner and Rebecca Wright. "Accountability and deterrence in online life." Paper presented at ACM Web Science Conference 2011, Koblenz, Germany, June 14-17, 2011.

Guagnin, Daniel et al., ed. *Managing Privacy Through Accountability*. Basingstoke: Palgrave Macmillan, 2012.

Haeberlen, Andreas. "A Case for the Accountable Cloud". Proceedings of the 3rd ACM SIGOPS International Workshop on Large-Scale Distributed Systems and Middleware. New York: ACM, 2009.

IBM. *The Enterprise Privacy Authorization Language (EPAL)*. 2003. http://www.zurich.ibm.com/security/enterprise-privacy/epal/. Accessed 28 February 2013.

Information Commissioner's Office. *Privacy by Design - Data Protection Topic Guide*. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_by_design.aspx. Accessed 28 February 2013.

—. *Privacy by Design report*. 2008. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx. Accessed 28 February 2013.

Jagadeesan, Radha, Alan Jeffrey, Corin Pitcher and James Riely. "Towards a theory of accountability and audit." Proceedings of the 14th European conference on Research in computer security. Berlin: Springer, 2009.

Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). *Break-glass: An approach to granting emergency access to healthcare systems*. 2004.

Karjoth, Günter, Matthias Schunter and Michael Waidner. "Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data". Proceedings of the 2nd Workshop on Privacy Enhancing Technologies, . Berlin: Springer, 2003.

Lazouski, Aliaksandr, Martinelli, Fabio and Mori, Paolo. "Usage control in computer security: A survey." *Computer Science Review* 4 (2010): 81-99.

Le Métayer, Daniel. "A formal privacy management framework." Proceedings of Formal Aspects in Security and Trust. Berlin: Springer, 2009.

Marx, Gary. "Privacy is not quite like the weather." In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert. Berlin: Springer, 2012.

Organization for the Advancement of Structured Information Standards (OASIS). *eXtensible Access Control Markup Language (XACML) Version 3.0 OASIS Standard*. 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf. Accessed 28 February 2013.

Organisation for Economic Cooperation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 1980.

—. *Thirty Years After The OECD Privacy Guidelines*. 2011. http://www.oecd.org/sti/ieconomy/49710223.pdf. Accessed 28 February 2013.

Park Jaehong, and Sandhu, Ravi S. "Towards usage control models: beyond traditional access control." Proceedings of ACM Symposium on Access Control Models and Technologies. New York: ACM, 2002.

Poullet Yves. "How to regulate Internet: new paradigms for Internet governance Self-regulation: value and limits. In *Variations sur le droit de la société de l'information*, edited by Claire Monville, Cahiers du Centre de Recherches Informatique et Droit. 79-114. Bruxelles: Bruylant, 2001.

Parliament of Canada. *Personal Information Protection and Electronic Documents Act*. 2000.

Raab, Charles. "The Meaning of 'Accountability' in the Information Privacy Context." In *Managing Privacy Through Accountability*, edited by Daniel Guagnin et al., 15-32. Basingstoke: Palgrave Macmillan, 2012.

Reed, Chris. "Taking Sides on Technology Neutrality." *SCRIPTed* 263 (2007):263-284.

Schneider, Fred. "Accountability for Perfection." *IEEE Security and Privacy Magazine 7* (2009):3-4.

Schneier, Bruce and John Kelsey. "Secure Audit Logs to Support Computer Forensics." *ACM Transactions on Information and System Security 2* (1999):159-176.

Title 12 of the United States Code. *Right to Financial Privacy Act*. 1978.

US Federal Trade Commission. *Fair Information Practice Principles*. 1973.

Trabelsi, Slim, Gregory Neven, and Dave Raggett. *PrimeLife Deliverable D5.3.4: Report on design and implementation*. 2011

W3C. *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*. 2006. http://www.w3.org/TR/P3P11/. Accessed 28 February 2013.

Waters, Brent, Dirk Balfanz, Glenn Durfee and Diana Smetters. "Building an Encrypted and Searchable Audit Log." Proceedings of the Network and Distributed System Security Symposium. Reston: The Internet Society, 2004.

Wright, David, Raphaël Gellert, Serge Gutwirth, and Michael Friedewald. "Minimizing Technology Risks with PIAs, Precaution, and Participation." *IEEE Technology and Society Magazine 30* (2011)*:*47–54.

Wright, David and Paul De Hert, ed. *Privacy Impact Assessment*. Berlin: Springer, 2012.