I. INTRODUCTION: WHO CARRIES WHICH RESPONSIBILITIES IN THE INFORMATION SOCIETY?

At Think Privacy, a public debate organized in the European Parliament on 28 January 2010, the following question was asked to the large audience: 'Who takes responsibility for his or her privacy: the government, the ICT companies or the Internet user, who distributes his personal details on social networking sites?' The question was raised after a presentation by Michel Walrave, professor at the University of Antwerp, presenting the results of research on teenagers’ online self-disclosure, showing that young people are aware of privacy concerns but in practice do little to protect their privacy. The public were first asked to vote on who was responsible, who then, and so on. The result of the vote is of no importance. What was striking was that the vote made an issue out of something that from a human rights perspective, allows for no such a choice (see below).

The voting game, making responsibilities look like options, is often introduced by representatives of industry and business. '(Security as a consumer choice'). We tend to see this as a strategic move to avoid a proper debate about the allocation of responsibilities. The voting game is reminiscent of the resistance to attempts by the United Nations (UN) to motivate international companies to respect human rights when they operate in countries with weak legal structures. International firms prefer the current status quo and to avoid certain answers to burning human rights issues.

In this contribution we will look at this UN debate, because it bears many parallels with our discussion about accountability in the information society (section 2). The Protect, Respect and Remedy scheme proposed by the UN Special Representative to the Secretary-General offers a solid framework for assessing the scope of duties that need to be taken care of in every human rights discussion about accountability. We then turn to European human rights law and its poignant answers regarding these responsibilities (section 3). Contrary to the international context of human rights protection, European human rights law with its insistence on positive duties to protect rights and freedoms such as privacy obliges every European state to take action whenever rights and freedoms are at stake. The state can do so by doing all the necessary work itself, or by making others take up their responsibilities (section 4-6). The concept of system responsibility is key to understanding the current accountability discussion in Europe. It is not only a moral, but also a legal concept, so do we believe, flowing from positive state duties in European human rights law (section 6). In some cases member states are mandated to implement new criminal law provisions (section 4).
The positive state duties are by no means vague (section 7-8). Judgments such as Gaskin, Peck and I. v. Finland are discussed with a view to understanding the concrete implications of the theory of positive human rights duties in the context of the information society (section 9-12). Through these judgments we learn a lot about the way a system of access to courts needs to be set out for victims of rights breaches in the information society. The legislator has a role in this, since he has to make access to justice possible. However, his responsibility goes much further. Applying the Protect, Respect and Remedy scheme we highlight the need to complement a scheme of remedies with pro-active regulation of the information society in order to avoid human rights violations. The contribution then considers how, with the EU Charter on Fundamental Rights and the series of amendments to the ePrivacy Directive, the European Union is showing the way (sections 13 and 15). These developments are elaborated with a consideration of how the debate around human rights and data protection in the face of consequential data processing technologies has developed and which problems it faces. It is demonstrated how a more nuanced understanding of responsibility allocation as well as human rights obligations also demands (and leads to) a more nuanced approach to the specificities of each technology (section 14).

2. RESPONSIBILITY FOR HUMAN RIGHTS VIOLATIONS BY MULTINATIONALS

2.1. Background

The United Nations is, as a promoter of human rights in the world, committed to the issue of human rights and corporations. In international human rights law states alone are responsible for complying with human rights legislation. Corporations are not (yet) regarded as having direct obligations. Consequently, it is the role of the nation states to oversee the conduct of corporations in their respective territories. In weaker countries, the conduct of rich and powerful multinationals, for several evident reasons, is not always easy to control.

Therefore, the United Nations aims to create an international initiative to support these weaker countries. One of the first United Nations initiatives to bring corporations in line with human rights was the UN Code of Conduct for Transnational Corporations. This project, which began in the mid-seventies, sought an overall regulation of the activity of transnational corporations and included a consideration of their human rights impact. The idea behind such a code has never been formally adopted by the United Nations and the project was stopped in the early nineties. In 1998, within the UN Subcommittee for the Protection and Promotion of Human Rights, a (sub) group of experts was set up, which established the ‘Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights’ (the Norms). This document represents a first attempt to establish legally enforceable human rights obligations for corporations and a move away from the traditional view that states have a primary responsibility for the protection and promotion of human rights. The Norms add to this the idea that companies have at least secondary responsibility in this regard. On August 13, 2003, in Resolution 2003/16, the Subcommittee adopted the Norms unanimously. They were subsequently discussed in March 2004 by the UN Human Rights Commission, where they were greeted rather coldly. The main discussion point concerned the mandatory nature of human rights obligations for corporations created by the Norms. Most Western states and most developing countries were, under pressure from the corporations, reluctant to impose legally enforceable human rights obligations on corporations. A solution to this deadlock was to
create yet another new initiative which consisted of appointing a Special Representative (John Ruggie, a US academic) with the task of examining the issue rights violations by transnational corporations again. In 2008 Ruggie presented his report *Protect, Respect, Remedy*, containing a description of ‘building blocks’ to bridge the so-called governance gaps in this area. Ruggie distinguishes three, different, but complementary, parts in his approach. First, the duty of the state to protect its citizens against human rights violations (Protect), second, the corporate responsibility to have respect for human rights (Respect), and third, the access to remedies when violations have occurred (Remedy).

### 2.2. ‘State duty to protect’, ‘corporate responsibility to respect’ and ‘access to remedy’

Ruggie’s first part deals with the duty of the State to protect individuals against human rights violations, including those committed by corporations. Ruggie returns to the classic idea within international human rights law making state protection the cornerstone of the legal system. The report emphasizes the importance for states to encourage and implement a corporate culture respectful of human rights. This requires a coherent government policy, greater cooperation with international bodies and initiatives, and special attention to conflict areas. It is emphasized that corporations can affect virtually all human rights.

The report then turns to the duty for corporations to respect human rights. What is needed in this discussion is to define the scope and content of the “responsibility” of corporations concerning human rights. A first obligation for companies is to operate in such a way that they comply with national laws, and generally avoid any human rights violations (do not harm). When, however a corporation operates in a country where no, or only minimal, human rights law exists, the corporation only complies with its responsibility to respect human rights if it acts with *due diligence*. This concept implies that diligent companies should ideally adopt and integrate a human rights policy, should carry out human rights impact assessments, and should subject their policies and activities to external audit and monitoring.

The third pillar of Ruggie’s human rights programme deals with access to remedial measures or remedies. Although in many countries a great variety of remedies exist - legal and non-legal – the access to legal remedies is often inadequate and non-legal remedies tend to be underdeveloped. To be effective and credible, the legal remedies must conform to certain principles. Thus, these remedies need to be legitimate and accessible to all and the procedure should be predictable, equitable, transparent and consistent with internationally accepted human rights standards.

The inaccessibility of existing mechanisms can be due to the lack of knowledge about them. Victims of human rights violations are often not aware of what remedial measures exist or and where to find them. Even when they find their way, the results are far from promising due to the, often limited, powers and scope of the existing reparation mechanisms. To remedy these shortcomings, the report suggests the creation of a global ombudsman, empowered to receive and process all complaints regarding human rights and corporations centrally.

Responses to the *Protect, Respect, Remedy* report were positive. The Human Rights Council, member states, corporations and civil society, … all gave the report a warm welcome. However, not all responses were equally positive. A group of NGOs requested that the Human Rights Council, in its new mandate, go beyond the Protect, Respect, Remedy framework, and also pay attention
to the liability of corporations for human rights violations. “In defining the scope of a follow-on mandate we therefore urge (...) to broaden the focus beyond the elaboration of the ‘protect, respect and remedy’- framework, and to include an explicit capacity to examine situations of corporate abuse. A more in-depth analysis of specific situations and cases is needed in order to give greater visibility and voice to those whose rights are negatively affected by business activity and to deepen understanding of the drivers of corporate human rights abuses. Both elements should underpin the elaboration of the framework and proposed policy responses. For example, the modalities of corporate impunity and its impact on the enjoyment and protection of human rights need greater scrutiny as an integral part of the effort to identify solutions. A cornerstone of human rights is combating impunity. To date the mandate has placed relatively little emphasis on the means of holding companies – including those that operate trans-nationally – to account. But for victims of human rights violations, justice and accountability can be as important as remedial measures” (emphasis added).”

2.3 SIX LESSONS FOR THE DEBATE ON THE INFORMATION SOCIETY.

The above provides relevant elements for the debate about responsibility in the information society.

1. There is, as above, a tension between ‘international players’ and ‘weak players’ in the discussion about the digital world. Strong, untouchable (American) players such as Facebook, Intel, Microsoft and Google operate from Silicon Valley where data protection laws are inferior to European standards from whence they so incessantly and metronomically bombard us with ICT solutions that no defence is possible.

2. Also apparent in the debate about multinational companies and human rights is the argument about the alleged market distorting effects of government intervention. The preceding paragraphs show that resistance against mandatory norms, which are imposed on corporations, comes from both Western states and developing countries. The belief that greater protection for the citizen kills a climate of innovation seems rife amongst policy and decision makers who would prefer not to regulate or to render immune the ‘vital forces of the economy.’ In the context of the information society we recall that the E-Commerce Directive provides a favourable liability regime for access providers (who transmit information) and hosting providers (who also store information). This regime purposely differs from the ordinary civil and criminal liability regime. The favourable regulation was created to specifically to make sure not to overburden this type of service with too many responsibilities.

3. The debate about multinational companies and human rights is not about whether corporations should commit themselves to respect human rights. We have seemingly and fortunately passed that phase. The debate is about the way in which corporations should show that commitment and, more specifically, whether there is a need for legally binding norms. Similarly, in the discussion about the Information Society, the debate no longer revolves around the question as to whether we are in need of human rights for the Internet or in need of values such as a ‘safe and reliable’ Internet. The debate has moved on (in the right direction) and concerns questions such as: ‘How are these values to be realised?’ and ‘Is there a need for “legally enforceable” rights or norms that determine who is primarily and secondarily responsible for potential problems?’ The
question about liability is therefore legitimate. Without defining responsibilities, governance gaps remain.

4. Within the accountability paradigm several choices are possible. In the debate about multinational corporations and human rights, Ruggie’s ‘Protect, Respect, Remedy’ scheme seems acceptable to most ‘stakeholders.’ However, some in the NGO world prefer to go one step further, especially when the responsibility of corporations is concerned. They advocate an ‘upgrade’ of corporate responsibility and a conversion from their respect-assignment into a protect-assignment. They advocate a shift from (mere) compliance to accountability.17

5. In the debate about multinational corporations and human rights, the weak (people in developing countries who ‘choose’ to work for multinational corporations, whatever the conditions are) are not held responsible for their choices and predicament. The existence of asymmetrical power relations allowing no freedom of choice for the weak is undisputed. Is it that different for a citizen in the Western information society? Are they capable of making the right choices when clicking and browsing? Research on the digital divide shows that each employee can be considered ICT illiterate five years after losing their job. The evolution is so fast that the loss of a lifelong learning environment is disastrous. Although it can be accepted that Internet users must have some responsibility, it seems unfair to make them the main responsible actor. Many Internet users are unaware of the small print privacy warnings and know absolutely nothing about invisible Internet protocols.

6. What the third building block of Ruggie’s Protect, Respect, Remedy scheme brings up well is that citizens should not be approached in terms of ‘personal responsibility’, but rather in terms of empowerment. If a citizen has responsibilities to bear, in a context where insecurity seems to be possible, then he or she should be given access to adequate legal and non-legal remedies (“access to justice”). In addition, the focus of awareness campaigns should not (exclusively) be on the individual’s own responsibility, but rather on the existence of such remedies and remedial measures, with the level of support necessary to envisage facilitating agencies such as the Ombudsman. Meijer, a Dutch author, calls these kind of arrangements ‘accountability arrangements’.18 In the Third World in general there are very few of these arrangements. Meijers suggests a similar situation in the West regarding eGovernment: Governments are indeed setting up front offices, serving the citizen using multiple back offices, but when things go wrong these front offices are more than often legally untouchable as accountability structures still focus on back offices.19 Hence, our duty is to focus the debate in the information society on clear accountability arrangements rather than proclaiming the death of privacy.

3. THE EUROPEAN HUMAN RIGHTS PERSPECTIVE ON RESPONSIBILITY IN THE INFORMATION SOCIETY

The European perspective on the liability and responsibility question is largely governed by the European Convention for the Protection of Human Rights (ECHR) (1950) interpreted and adapted to modern contexts by the European Court of Human Rights, sitting in Strasbourg and (to a lesser extent) by community law and the EU Charter for Fundamental Rights (2001) interpreted by the Court of Justice in Luxembourg. We note in passing other human rights texts such as the 1990 Convention on the Rights of the Child and the Additional Protocol to that convention,
which includes one specifically relevant provision stating that children have a right to privacy. However, in this contribution we will confine ourselves to Europe and especially to the progressive and encouraging work done by the European Court of Human Rights (ECtHR).^20

Formally speaking, the European human rights text is as traditional as other international texts in the sense that the text is directed at member states and does not impose directly binding obligations to corporations or individuals.^21 However, the European Court has caused a breakthrough with the development of the doctrine of positive obligations.^22 This doctrine, also recognised in comparable supra-national systems, but absent in others, e.g. U.S. constitutional law, was developed by the European Court with a view to evaluating government behaviour in complex cases.^23 Take for instance the case where the rights of an individual are not threatened by a specific concrete action on the part of a government official, but by the non-movement or inaction of the government. The doctrine allows the potential condemnation of the state for the failure to have taken appropriate action in line with their obligations to ensure the enjoyment of the right.

The doctrine has so far been applied in relation to many rights enshrined in the Convention (e.g. the right to life protected by Article 2, but its main applications so far concern the rights protected by Article 8 of the ECHR. Article 8 ECHR recognizes the rights of the protection of privacy, family, communication and home. On the basis of the doctrine, this provision not only prohibits the state from interfering in the rights of citizens, but it also includes an obligation for state parties to adopt measures to ensure the effective enjoyment of the privacy right or any other right under Article 8 ECHR and to introduce specific provisions to prevent or punish the acts of individuals who would ignore or violate these rights.^24 Although this ‘positive’ duty is not expressed as such in the treaty, it has been inferred from it by the Court.^25

The first Article 8 ECHR application of the doctrine was in the Marckx case (1979) and the Airey case (1979) on the right to family life and also the judgments Rees (1986) and Gaskin (1989) concerning the right to private life.^26 More recently, the doctrine of positive obligations was applied in the Stjerna case (the right to alter names)^27, the Guillot case (naming)^28, the Willsher case (access rights)^29, the López Ostra and Guerra (environment) cases^30 and in the Botta case (disabled facilities).^31 We will come back to some of these cases below.^32

In the Botta judgment, the Court clarified that it is up to the Court to decide if there is (or if there is not) such thing as a positive human rights duty and it will only acknowledge the existence of such a duty “when it considers that the measures requested by the person are directly and immediately linked with the private and family life of the person concerned.”^33 In last instance it is therefore the Court’s decision to determine whether a positive obligation exists or not. It is therefore not possible to establish a precise index of positive duties, nor is it possible to determine in advance which initiatives a state needs to take to effectively respect private and family life.^35

Decisive in developing this revolutionary doctrine was the 1979 Marckx ruling. In the Court’s view, the right to respect of family life does not only result in a duty for the government (continued) to refrain from interfering in family life, but it also results in a positive duty. Because of the right to protection of family life, states should especially take those measures that are necessary to make this right possible. As such the existence of positive obligations in relation to family life implies that when states develop family law rules, these should not impede on the normal devel-
opment of family relationships, but, on the contrary, should provide the context to make their enjoyment possible.

In 1979 the Court ruled on the impossibility for Mrs. Airey to be able, on the basis of Irish law, to file for divorce. For the claimant this legislation constituted a breach of several fundamental rights. One was the fundamental right to the protection of privacy and family life. The Court saw no negative duty breach (the negative duty not to infringe), but discussed the case in terms of positive duties. Mrs. Airey’s core complaint was not that Ireland had performed an act, but rather that it failed to act. In the rest of the judgment, the Court then turned to the analysis of this positive duty. Should Ireland have altered its divorce laws to make them more flexible in light of contemporary human rights standards?

In identical terms and with reference to the Airey principles, the Court ruled in the Gaskin case (1989) that the refusal of UK authorities to give Gaskin access to a file on his childhood years is not to be understood as a violation of a negative duty. The British government officials did not really do anything detrimental with Gaskin’s data, but simply refused him access. This cannot be considered as a violation of a negative duty. However, it can be possible to look at the facts as demonstrating non-compliance with a positive duty on the part of the British government to meet Gaskin’s request.

4. POSITIVE HUMAN RIGHTS DUTIES AND PROTECTIVE CRIMINAL LAW PROVISIONS

The standards set out by the European Court are high. States can even have a positive human rights duty to single out certain acts as crimes and the Court has accordingly extended the doctrine of positive state obligations to criminal law. Sometimes this doctrine implies that additional criminal legislation is necessary in a member state. Distinctive is X and Y v. Netherlands (1985), concerning the application of the doctrine of positive obligations to the problem of protecting the public from sex crimes. In this case the Court condemned the Netherlands, because its legislation did not allow the prosecution of someone who was sexually violent towards a mentally handicapped girl who had just turned sixteen.

Marckx and X and Y v. Netherlands teach us that there are at least two kinds of positive obligations in European human rights law. States need to take measures that make the exercise of fundamental rights possible, and need to introduce specific provisions for the prevention and/or punishment of acts of individuals who ignore or violate basic rights or obligations. This broad set of duties plays a role in MC v. Bulgaria (2003). The Court found a violation of the treaty because M.C. – a victim of rape - was not legally protected in Bulgaria in a satisfactory way. Not prosecuting in a case of rape is a violation of the positive obligation of a contracting state to protect its citizens against violations of their fundamental freedoms and rights through an effective legal system and to investigate complaints thoroughly. From M.C. v. Bulgaria one can also infer a duty to reasonable and adequate criminal law making.

To these duties (to enable enjoyment, to investigate certain complaints and to protect through criminal law), one must add the duty to ensure an effective remedy for human rights abuses as laid out in Article 13 ECHR. This right is considered a necessary complement to the other treaty rights. Citizens not only ‘have’ the regular rights (the right to privacy, to life, to freedom of expression etc.), but they also have the right to an effective remedy when these rights are violated.
5. RESPONSIBILITY AND ITS DISTRIBUTION AMONGST STAKEHOLDERS

This brief discussion of the Strasbourg machinery and the European doctrine of positive state duties to realize effective enjoyment of rights gives a new meaning to the old rule that the ultimate responsibility for human rights violations lies with the state. In a certain way the old rule applies more strictly than ever before: human rights violations by non-state actors can trigger state responsibility when certain positive duties have not been adequately met. States have final responsibility for human rights violations within their jurisdiction. This responsibility is a source of specific duties. These duties relate to the three building blocks identified by Ruggie: Protect, Respect and Remedy. By creating a protective environment by making non-state actors directly accountable to human rights standards and by installing effective remedies for redress, states can defer this responsibility. Putting pressure on companies through administrative law or human rights law (‘sharpening accountability, or increasing ‘enforcement’ on ‘compliance’), creates liability immunity in Strasbourg. A legal system cannot guarantee that no human rights violations occur, but efforts need to be taken to prevent them and when they occur the system needs to be responsive.

A translation of these human rights duties to the information society context is not difficult. Of course not all the judgements discussed above relate to the information society, but at least in our view, enough guidance is given for states to take up their duties with regard to the Internet and other modern media.

It is not only about non-interference, but about the full package: to protect, create respect and to remedy. More specifically, governments must protect their citizens against human rights abuses by companies and against abuses by other users on the Internet (first building block); ensure that companies respect their human rights obligations (second building block); and provide easily accessible remedies or remedial action (third building block).

Concerning the second building block, the government may choose (consciously or by not acting), to be lenient towards ICT companies and service providers, but this may amount to a neglect of the duty to protect and the government will then be held responsible in Strasbourg for possible human rights violations committed by third parties. Alternatively a government may choose to distribute responsibilities by tying ICT companies and service providers to certain satisfactory standards. In the case of possible violations, the Strasbourg test would be less painful. Making private actors more accountable helps governments to respect contemporary human rights standards.

6. SYSTEM RESPONSIBILITY AS A LEGALLY BINDING ACCOUNTABILITY SCHEME

Calls for accountability fit well in a postmodern digital age where traditional power structures, such as oversight by parliament, are losing their importance and where complex and rapidly evolving global and technological processes often preclude solid and effective anticipatory regulation via legislation and government policy. Meijers, who distinguishes between liability (limited, only relevant in disputes) and responsibility (all encompassing), correctly identifies a double accountability scheme for governments in the digital era. Next to the responsibility for their own services and actions, states now have broader system responsibility that extends to all use of ICT, regardless of by whom in any given society.
As regards the responsibility of use by the government for its own applications, accountability has a rather natural place - which does not mean that it is always provided. Through accountability arrangements, the inevitable uncertainties associated with the introduction of new systems can be dealt with, to a certain extent, by anticipating on an institutional level, that there will be problems and disputes. System responsibility (for technological developments outside its own organization), on the contrary, triggers a different kind of accountability. Now, the government is, as it were, on the side of the individual citizen in demanding the accountability of service providers in the ICT market. This is, seen from the government’s perspective, a more difficult role than setting up accountability in their own processes. This broadened role is ambitious and complex. It forces governments, amongst others, to take action in order to protect citizens against identity theft, to organise appropriate forums for conflict resolution and to introduce protective conditions for the freedom of expression in the light of the existence of actors on the Internet that have excessive social power.

A human rights law analysis, like the one proposed in this paper, adds more body and colour to the important idea of system responsibility. System responsibility is neither an ideal nor a virtue nor a voluntary option for the wise policy maker, but legally imposed starting point for regulation. Part of the system responsibility consists of making actors such as internet companies comply with human rights standards. Governments simply must support citizens in demanding accountability. Governments are not directly responsible for every human rights violation in their jurisdiction, but they are obliged to ensure that through the efficient distribution of responsibility, responsibilities are covered.

7. POSTMODERN VAGUENESS AND LACK OF CLEAR ACCOUNTABILITY SCHEMES?

Meijer quotes many ‘governance’ authors announcing the end of traditional Westphalian state sovereignty and pointing out the failures of the traditional idea of ‘government’. Developments in technology and globalisation undermine the essential traditional pillars (territoriality and the absence of a role for external agents) of Westphalian state sovereignty. The collapse of the nation state makes traditional law mechanisms obsolete. The question then arises as to whether law can still play a meaningful role in this context?

Most lawyers have never been able to fully understand that question. For them, law is an activity or a procedure, rather than a norm setting system, a process more than an institution or structure. Law in this view is to be compared with a signalisation system that attributes facts and events to persons or legal actors. By speaking the law and operating legal principles of attribution judges do no more than apply, construct and maintain a system of responsibilities. All kinds of legal systems coexist within and outside of the state. Sometimes people have a choice and they can do legal forum shopping. Do we take this damage to a criminal court or to a civil court? Do we go to the Court of Justice in Luxemburg or do we stick to a national court. Law reinvents itself constantly. Leaving behind traditional and strict liability mechanisms from private law and tort law, Strasbourg seemingly develops a liability system that is modern in more than one way: If there is a complaint about a human rights violation in a certain state, then that specific state is accountable. Governments of European states will be held responsible in Strasbourg when their own actions amount to human rights violations, when inaccuracies or errors are found in their accountability arrangements or when there is no, or a careless, distribution of responsibility.
We contend that this human rights accountability system is a significant (but of course not sufficient) response to the alleged deficiencies of the classical Westphalian legal system.\textsuperscript{57} Meijers discusses the fact that most Internet users do not understand the invisible protocols of the Internet\textsuperscript{58}, and that through the use of information technology the anatomy of decisions is obscured with the result that certain governmental acts are less open to contention.\textsuperscript{59} Strasbourg simply shrugs its shoulders and turns to the one stakeholder that is always identifiable: ‘the’ government of a member state. It will be this government that will be held accountable for violations of privacy and other rights when scrutiny reveals that no satisfactory legislative or regulatory initiatives have been taken to protect these rights of the citizen or when insufficient accountability arrangements have been created in the light of the right to an effective remedy. How so postmodern vagueness and lack of clear accountability schemes?\textsuperscript{60}

**8. CONCRETE CONSEQUENCES OF SYSTEM RESPONSIBILITY**

The story of globalisation and complex technological developments brought to us by serious scientists is one that politicians often play out strategically to shift away their system responsibility (‘Things are not in our hands, and the Americans do not listen!’). Our human rights analysis gives a much more pressing account. The recognition of system responsibility in Strasbourg explains why there is, in Europe at least, no accountability without the sanction of liability. The challenge is to understand how far these positive obligations to system responsibility stretch. In general the answer is not too far. The broader, state accountability, scheme is only triggered when positive duties are recognized, and European courts are prudent when recognizing extensive state duties. Too prudent, if we are to believe many authors that single out the limited extra value of the positive duty doctrine for citizens and vulnerable groups in particular. In an article from 2005, Olivier De Schutter highlighted the missed opportunities in the case law of the European Human Rights Court to provide for real protection and identified certain structural and institutional limitations to court procedures to further develop human rights law.\textsuperscript{61} Too often judges prefer to work with open concepts and avoid more general statements that make duties concrete. The outcome of their cases is too closely linked to the immediate context of the claimant. More fundamental is De Schutter’s observation that the ‘binary’ character (all or nothing) of the judicial function often leads judges to a hands-off approach.\textsuperscript{62} Clearly we cannot entrust the difficult task to identify positive human rights duties to the judges alone.

The concrete shape of a privacy policy that a corporation is obliged to develop in the name of human rights will have to be determined using other sources, in particular by law. It is probably not fair to demand a high level of detail from Strasbourg. Understanding the full implications of our commitment to human rights is not the sole responsibility of the European Court. Human rights are primarily the responsibility of member states that recognise them.\textsuperscript{63} It is the responsibility of our governments to think through the idea of negative and positive obligations in the context of the information society.\textsuperscript{64} The European Court will only reluctantly position itself thusly, preferring to avoid substituting itself for elected authorities mandated to make certain choices depending on factors such as budgetary constraints. The Court will however look at the outcome of these deliberations to safeguard treaty rights that need to remain practical and effective.\textsuperscript{65} The European Court is becoming more active and clear in recent judgments on the issue of positive state duties in the context of the information society. In the following, we will discuss
some of these important judgments. They will aid understanding as to the extent of the system responsibility that authorities should shoulder.

9. SYSTEM RESPONSIBILITY CONCERNING ACCESS AND PUBLIC PRIVACY: GASKIN AND PECK

Already in 1989, with the Gaskin case (which was discussed above), the Court had made perfectly clear that the theory of positive obligations was of a significant enough nature to alter our understanding of privacy obligations. The Court ruled that the act of not allowing access to a person’s data violates the Convention. To have access to one’s data is an aspect of the right to privacy that entails a duty to others to allow this access. In the name of privacy, access should be given, even when national law contains no explicit provision in this regard.

Does the foregoing mean that no national legal basis for the right to access rights needs to be created? Does recognition by Strasbourg of a (human) right to access make national legislation creating such an access superfluous? On the contrary, national governments should make policy in advance. The Strasbourg system is not meant to be a permanent backup system (see the principle of subsidiarity, above). The Court merely helps the member states to understand the scope of the rights agreed upon and to regulate accordingly.

It is useful to add to this the observation that the European Court is not to be compared with a regular constitutional court that is mandated to check the validity of legislation. A case can only be taken to Strasbourg when there is a concrete violation of rights and an individual claims status as a victim. A claim that there is a problem solely based on the observation that, for instance, national law does not regulate CCTV, would not be admissible in Strasbourg, hence the obligation to wait for a real camera problem before going to Strasbourg.

Interestingly, for our understanding of the information society, this did not happen until late in the history of CCTV. In the Peck case, CCTV-images were made of a suicide attempt in a public place. The images from these CCTV cameras were made available to journalists and shown on British television. The Court condemned this practice: Publication, through media outlets, of sensitive data is in this case a breach of Article 8 ECHR; the fact that the claimant was clearly recognisable on television and the publication of his picture in the press constitutes a violation of his right to privacy. The right was violated as the data subject did not give his approval, nor was he made unrecognisable.

Peck is important because it removed the last doubts for certain stakeholders, who up until 2002 had been ignoring the human rights dimensions of CCTV. The judgment illustrates the broad meaning given by the European Court to the right to privacy. The view that everything we do in public is automatically unprotected is simply incorrect in Europe. The Court recognises the applicability of the right to privacy for acts outside the ‘strict private sphere’ and involves in its analysis, inter alia, the criterion of reasonable privacy expectations. Translated into the context of social networks, this means that our right to privacy is not lost forever because we share information with others, especially not if we have the expectation that the person(s) responsible for the social networking site handles our data responsibly.
10. SYSTEM RESPONSIBILITY CONCERNING SECURITY: I. V. FINLAND

In 2008, twenty years after Gaskin, a new dimension was added to the doctrine of positive obligations in the context of the use of personal data in I v. Finland. The Court ruled that the security measures taken by a Finnish hospital - measures that when implemented properly could have guaranteed the right to respect for the private life of an HIV patient who worked at the same hospital - were inappropriate and found a violation of Article 8 of the ECHR.

In its approach to the case, the European Court identifies some general principles relating to personal data. Medical information falls within the scope of Article 8 ECHR: “The protection of personal data, and specific medical information, are fundamental to the right of a person to respect for his / her private and family life.” The Court also recognises that the most important - negative - object of Article 8 protection consists of “protecting individuals against arbitrary interference by public authorities”, but at the same time emphasizes that there are positive obligations that may derive from the right to respect for one’s private life. These obligations include the adoption of measures, which can ensure the right to respect for private life, even when these rules apply to relationships between individuals. The Court observes that the protection of personal data, especially that of health data, is fundamental for the right to protection of privacy and family life on the part of the patient.

Such protection is not only crucial to respect the feelings and expectations of patient privacy (“the sense of privacy of a patient”), but also for patient confidence in the medical professions and health services in general. Positive obligations concerning care for personal data do not merely serve individual interest. There is a general interest in protecting confidentiality. This duty may also be required from private persons.

After listing these general principles, the Court turns to the relevant Finnish law. Article 26 of the Finnish Data Protection Act (‘the Personal Files Act 1987’) requires the processor of personal data to take security measures and to ensure that only treatment personnel have access to files. Strict application of this provision would have been an effective protection under Article 8 ECHR and would have allowed the hospital to control the access (“to police strictly access to a disclosure of health records”).

In the Court’s view there was no adequate security in place, which amounted to a breach of the Finnish Act and consequently to a violation of the ECHR. The taking of security measures by companies and institutions such as established in data protection legislation, does not constitute merely a moral or a simply legal obligation, but must be seen as a positive human rights obligation. Failure to comply with that requirement is therefore equated with a violation of the Convention. Further to the above violation: it was also found that there was neglect of the human rights duty to investigate.

In sum, what is needed, according to the Court, is practical and effective protection to prevent any possibility of unauthorized access. This protection was not given here.

Dealing with personal data by individuals and institutions requires adequate security measures, with the purpose of guaranteeing the right to respect for private life. More generally, it can be said that by complying with existing legislation on data protection in the member states, the positive obligations which derive from the ECHR, are met.
discussion about vagueness surrounding the theory of positive human rights duties (*above*), we note that the section in the judgment containing ‘general principles’ proves to us that the judgment is relevant for more than just this individual (very sad) case. This is not the only European judgment with a section devoted to general principles. In more and more judgments the Court opens with an analysis of the applicable general principles, which are then taken as guidelines. This methodological rupture with traditional casuistic approaches of administering justice, aims to make possible further guidance to member states with a view to allowing them to adapt to the standards of the Convention as developed by the Court. In addition, we see in *I v. Finland* how the Court relies on data protection law and its extensive set of specific rights and duties. These are identified as positive human rights obligations. Data protection legislation is not mere legislation. It is warranted by our human rights! Data protection laws after *I v. Finland* can be considered as checklists for positive human rights obligations.

11. REMEDY AND FINANCIAL COMPENSATION CANNOT BE THE ONLY BUILDING BLOCK

In *I v. Finland* one can discern additional guidelines related to positive state duties, this time with regard to the ‘Remedy’ building block. Not every legal redress system is good enough for a law abiding information society. Finland got a serious reprimand for its system. The claimant complained about the way in which compensation was handled in Finnish law. She lost her data protection case because she failed to demonstrate a causal link between the deficiencies in access rules and the improper dissemination of information on her medical condition.

Lawyers recognise this situation. Damage is not enough in continental civil claims. Next to showing injury a person pretending to be a victim has to establish a causal link between the harm and actions or non-actions of third parties. The European Court is obviously not charmed by the stringency of Finnish civil law requirements. Placing such a burden on the shoulders of the claimant is unfair - the Court found: “To place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital’s record keeping at the material time.” If the hospital had carried out greater control of access to health information, for instance, by only giving access to those directly involved in the treatment, or by keeping a log book of all persons who had access to the data, then the claimant would have been in a less unfavourable position before the national courts.

In the information society where all processing of data leaves trails that can be checked on by the processor, it is unfair and contrary to the Convention to expect significant proof from the data subject, who does not control the computer but is simply being registered in it.

A feel for the practical obstacles faced by privacy victims is equally present in the Court’s position with regard to the question of how compensation for the claimant should be calculated. In practice, this is a thorny issue for regulators. What is the harm if one is careless with how personal data is handled? Privacy victims seldom die. In the present case, a person lost her job and reputation, but very often the damage is less evident. What is the damage when Sony loses billions of *Play Station* users data (including credit card data) as happened in early 2011? Does it make sense to go to court immediately or does one need to wait until further damage (monetary loss by misuse of credit card data) occurs? Having sloppy security measures is clearly a data protection error, but is it enough to warrant claims for compensation?
We would argue yes, but the Courts are seemingly not ready to go along with this to any significant extent. *I v. Finland* does not answer all questions, but the Court does underline that the applicant is also eligible for reimbursement for non-pecuniary damage. The claimant had suffered non-pecuniary damage and therefore qualified for financial compensation. “Failure to comply with a security requirement is not compensated by simply adjusting their security measures, but requires financial compensation.”

The importance of *I. v. Finland* for the discussion about the establishment of the information society is still raised too little. Its paragraphs are rich and complete. The ideas and guidelines about compensation that we discussed above are followed by complementary statements about the limits of compensation possible from a human rights perspective. Indeed, after having recognized compensation for pecuniary and non-pecuniary damage, the Court continues its reasoning by declaring that the mere fact that national legislation allows for compensation after privacy suffered damage is insufficient. The government should ensure a practical and effective protection of this right. Providing a system of compensation (Ruggie’s third building block) is therefore not enough. A society must do more work to achieve human rights standards. There should not just be legal settlement afterwards (when problems occur), but there should also be a clear set of guidelines in legislation and proper enforcement of these guidelines (to avoid problems). This does not mean that Ruggie’s third building block is unimportant. A system of compensation for damages must exist and must be based on fair and accessible procedures. No unreasonable burden of proof should be placed on the shoulders of the claimant and monetary compensation should be provided.

### 12. IF COMPENSATION IS AWARDED THEN IT MUST BE BOTH REASONABLE AND SUBSTANTIAL

Let us dwell a little longer on the issue of compensation. Some on the business side or on the governmental side will object to the foregoing: Where is it heading if, for violations of rules on use of personal data, we also have to compensate for non-pecuniary damage suffered? What are the limits of such an obligation? For the European Court, such compensation needs to be reasonable or proportional. The requirement that the compensation for abuse and accidents with personal data has to be reasonable is developed in *Armonas v. Lithuania* (2008). The facts of the case and the position of the Court are of such a nature that they give the daily reports in our newspapers about “accidents” with personal data (lost, press leaks, etc.) a special dimension. Armonas was married to L.A. who died on April 15, 2002. On January 31, 2001 Lithuania’s largest newspaper reported about a so-called Aids-threat which was prevalent in the region. The front-page article mentioned L.A. by name and surname and identified him as an AIDS patient. The article also reported that he had two illegitimate children with a woman, G.B., also an aids patient. L.A. starts proceedings against the newspaper and is awarded a small compensation for violation of his privacy. Lithuanian law places upper limits on compensation granted. Due to these restrictions in law the compensation could not legally exceed LTL 10,000 (about € 2,896) and L.A. (who died) received only very little compensation.

L.A.’s wife turned to the European Court with the complaint that her right to privacy had been violated because of the ridiculously low compensation that was granted to her husband, despite the recognition by the Lithuanian court that a violation of privacy had occurred. Such low compensation would not satisfy the requirements under Article 8 and 13 ECHR to provide an effective remedy.
Technically-speaking it was not certain that her case would stand up to scrutiny but the European Court declared the complaint admissible. This is usually a sign of the willingness of the Court to take the case seriously. Again, the starting point for the Court is the idea that negative and positive obligations are incumbent on States. The latter may include obligations for the government to take steps to protect the privacy in relationships between individuals. Proportionality is a central concept in assessing the scope of these obligations and in this case a fair balance had to be found between press freedom and the right to private life.

The publication of information on the health status of Armonas’ husband did not contribute to the public debate and only served to fulfil the curiosity of particular readers. The balance in this case therefore weighs in favour of the individual right to privacy. The government has an obligation to ensure that this right can be enforced against the press. The Court attaches particular gravity to the assertion in the article that the staff of the local AIDS centre had confirmed the information on L.A.’s health status to journalists. This, according to the Court, could be discouraging for others to take a voluntary AIDS test. The protection of personal data in this sensitive context is of particular importance.

In theory such a protection exists through Lithuanian data protection law. Also, compensation was awarded to L.A. The question, however, is whether the amount of compensation was proportionate to the injury and to what extent the legal provisions restricting the compensation to a fixed (low) amount were in line with Article 8 ECHR. It is not for the European Court to require that member states impose heavy sanctions. The Court leaves certain discretion in hands of the state concerning the regulation of financial compensation. They can take the socio-economic situation of a country into account and have to prevent overly heavy restrictions on the press from resulting in the right itself being eroded. Imposing overly heavy sanctions on the press can have a chilling effect on press freedom.

However, in case of a manifest abuse of that freedom, as in the present case, the Court considered that the heavy legal restrictions on the compensation of victims and the subsequent low compensation amounts were not in line with the expectations people have in that area in accordance with Article 8 ECHR. Therefore, there was a violation of Article 8 ECHR and Lithuania was held accountable.

The ruling Armonas v. Lithuania from 2008 indicates that not everything may be written in a newspaper. The lessons can be extended to other media such as the Internet. The distinction between the actual distribution of information as part of public debate on the one hand, and distasteful allegations concerning the private life of a person on the other is equally applicable. The government should protect its citizens against distasteful unwarranted allegations and citizens, bloggers or newspapers should refrain from publishing such information. Armonas also contains a fine illustration of the positive state duty to protect human rights (such as the right to data protection) in an alert and appropriate way, if necessary through the imposition of sufficiently high compensations in case of infringements by publishers, advertisers and media companies. Furthermore, this compensation needs to be proportionate to the suffered harm, and cannot be too low. States should set up their compensation system in such a way that restitution for harm is possible without an excessive burden of proof and there is no sham justice in the form of derisory compensation. An effective remedy as warranted by Article 13 of the Convention should be available, even when confined to cases with only mere moral harm resulting from a lack of respect for an individual’s right to self-determination.

In what follows, I will discuss the tasks of the legislator in the information society. It is clear from the above that our society not only needs to work on access to justice, but should also design and implement a system of legal protection and supervision in advance.
13. THE EU CHARTER: A CORNER STONE FOR SYSTEM RESPONSIBILITY

The EU Charter of Fundamental Rights, which was proclaimed on 7 December, 2000 and 14 December, 2007, was made legally binding for member states via the Treaty of Lisbon. This new human rights text not only repeats the contents of the ECHR, but also codifies new developments in human rights. Article 7 of the Charter provides us with the right to privacy, whilst Article 8 of the Charter goes a step further than the ECHR and recognises a separate right to the protection of personal data. The provision says that personal data should not only be protected but also that personal data must be processed fairly, that data must be processed for specified purposes (purpose binding), that personal data must be processed with the consent of the person or that personal data must be processed based on some other legitimate basis laid down by law. Article 8 of the Charter then goes on to grant each person access to data collected about them, a right to have this data corrected if needed and the right to be assisted by an independent controlling data protection authority (DPA) to oversee the compliance with the law.

Article 8 of the Charter can be understood as a corner stone for the regulation to be set up in Europe. It leaves no doubt about the need to protect all personal data and usefully recalls the existence of several important principles that govern all processing of personal data. In particular, the inclusion of the purpose limitation principle deserves credit. Its enforcement has very serious and widespread implications, for instance, for the work of the justice system and the police, for the actions of controlling employers and for social network providers that like to use their users’ data for new purposes other than those for which the data were originally collected, preferably without any transparency or consent. This principle is poorly anchored in Asian and U.S. law, which creates a lot of confusion with regard to transnational transfers of data and shared security initiatives such as PNR and Swift. From a European perspective, there is thus little harm in emphasizing its importance in a high visibility text. The same applies to another sore point in transatlantic relations, the question as to whether an independent supervisor, which would sanction and control the use of personal data, must be instated in a legal system.

The inclusion of these data protection rights and principles in the highest fundamental rights is not without significance, as the U.S. experienced recently when the European Parliament opposed access to SWIFT banking data due to lack of accompanying guarantees.

14. WHY SPECIFIC LEGISLATION FOR BIOMETRICS IF WE HAVE DATA PROTECTION PRINCIPLES?

The necessity of regulating technologies to avoid human rights issues has always been disputed and indeed for a number of reasons. Today this position is losing momentum, but there remain voices opposed to the detailed regulation of specific technologies. One opinion is that there is already enough regulation. The argumentation is that the protection of personal data has the best chance of success on the basis of existing general data protection principles that apply to any technology that processes personal data. These principles - the right of access, rectification and erasure, the purpose limitation principle, etc. - are contained in a set of well known international and European documents and legal instruments: the OECD Guidelines, the Council of Europe’s Data Protection Convention 108, the European Directive 95/46/EC and Framework decision 2008/977/JHA. The argument is then that we need no more. The general recognition that the already existing data protection principles apply to a new technology will do.
Surprisingly many advocate this view within and outside the EU. Within the EU this explains why no specific regulation has been elaborated concerning CCTV, although many citizens would agree with the view that this is consequential technology requiring more detailed regulation. Some seem to fear to be curtailed when more is done than just recognizing the applicability of very general principles to a specific technology such as CCTV. Others from within the data protection community fear that new regulations will be accompanied by serious limitations to the general principles. More regulation would then mean less protection.

Within both views the existence of general data protection laws is used to oppose data protection initiatives. The argument ‘we do not need regulation’ is traded in for the better sounding argument; ‘we do not need extra and more detailed regulation’.

Sticking to the general principles when confronting new technologies disregards the particularities (in terms of human rights consequences) of each specific technology. An image, for instance, is different from a written document on a person and a fingerprint is different again. It is, moreover, contradicting the pivotal Article 5 of Directive 95/46/EC which contains the rule that member states should actually indicate, with precision, the conditions under which the processing of personal data is lawful. In the absence of specific legislation on new technological developments, with clear conditions and limitations, the fundamental principle of fair and lawful processing remains vague and difficult to enforce. One must only think of the wide variety of biometric applications that exist and how their application varies across different actors (from swimming pools to border checks). In this light, how do you materialize these general principles of data protection?

European data protection law has therefore a duty to itself to actively protect European human rights. To proclaim that the Internet is unsafe and that surfing on it is at your own risk is not an option. The biometrics case and the somewhat older CCTV case are examples of technological developments past their initiation phase where almost all countries as well as the EU have missed a beat by not taking up their human rights duty to regulate. None of the three building blocks are there.

In many of its legal instruments there is some attention given to the three building blocks. The EU legal instruments on new technologies such as the proposed regulation for a European processing of passenger data include the ‘usual data protection rights’ such as the right of access, rectification, and erasure. However they seldom include strict deadlines within which these requests must be met or fulfilled. Equally, these regulations mention, as a rule, a right to compensation and a right to judicial remedies for any breaches, yet the scope of these rights is left to the scrutiny of the national legislators. In practice the added value is very limited, since the absence of strict rules on the liability of the different authorities involved does not allow the competent judicial or administrative authorities to impose sanctions when necessary.

The EU is, however, getting better at the regulation of other types of technologies and is increasingly living up to human rights expectations. Governments actively regulate many aspects of these new technologies. In fact the model of regulation is increasingly becoming the model of regulation our society developed for traffic regulation. No detail is ignored and there are rules for cars, drivers, signs and rules, the pavement and lighting. The ultimate aspiration of traffic regulation is to have safe traffic. Courts will use civil law provisions to address governments when it appears that, for example, traffic signs are insufficient or accidents are happening as a result of inadequate road surfaces.
Comparing cyberspace with traffic is an elegant way to signpost the direction we must head: A safe and reliable, human rights-friendly information society with a government that has final responsibility and regulates and actively delegates responsibility. A good example is the data protection policy, which the EU pursues in the telecommunications sector. The example that will be discussed in the next section illustrates that Europe has never hesitated to materialise the “sacred principles of data protection,” and to call risks and solutions by their true names. It is deplorable however, that the exercise has not been sustained across all technologies that have been launched in recent years.

15. AN ACTIVE APPROACH TO TECHNOLOGY: THE EXAMPLE OF THE EPRIVACY DIRECTIVE

Less than two years after the general Directive on the protection of personal data, the European Directive of 15 December 1997 concerning the processing of personal data and protection of privacy in the telecommunication sector was enacted with a view to complementing the general framework of 1995. This specific regulation ensured the protection and confidentiality of personal data processed by telecom services and networks. The directive focused heavily on ISDN technology. The lack of harmonization in this field would have disturbed the creation of a single market in the field of telecommunications. ISDN was therefore seen as an important pre-requisite for the further development of the internal market. The directive gave citizens important safeguards (in the form of new explicit subjective rights), including the creation of member directories and the installation of detailed bill and call forwarding. The directive also included numerous other new telecommunications safeguards. Member states are required by the directive to ensure that the confidentiality of communications via the public telecommunications network and publicly available telecommunications is guaranteed.

New rights were created with regard to number identification and rules were incorporated with regard to sexual and other malicious ‘breathing calls’. A first ban was introduced for providers on telecommunications services preventing the sharing of subscriber data, and a second ban concerned unsolicited spam. Automated calling systems for direct marketing were only allowed if subscribers gave prior consent.

The first ePrivacy Directive focused on public telecommunications networks (ISDN supported) and public digital mobile networks. The Internet was neither named in the text of the directive, nor in the preamble. To address the challenges posed by the Internet, the European legislator replaced the 1997 regulation by an updated version in 2002. This time the Internet and its challenges (cookies, spyware, malware and viruses) are clearly addressed to the benefit of the Internet user.

The story does not stop here. The 2002 ePrivacy Directive was again updated in 2009 to address further new developments. The object of the update illustrates an attempt by the legislator to distribute responsibilities to certain stakeholders in the telecommunications industry and to make them shift from compliance to accountability.

Firstly, the 2009 ePrivacy Directive obliges telecom companies to report security breaches of personal data (Data Security Breach Notification). It is in fact a double obligation. There is the obligation to notify the competent authority of every security breach, regardless of whether there is a risk to individual users. The notification must contain a description of the consequences of the violation and of any measures taken or proposed to address the violation. There is also an obligation to report to the individual users and to inform them of “likely adverse effects” on their
personal data and privacy. Consideration could be given to identity theft or fraud, physical harm, significant humiliation and loss of reputation. Telecommunications companies are required to keep an inventory of breaches, in which facts, consequences and remedial measures are recorded.

Secondly, there are new refinements in the rules about cookies, spyware, malware and viruses.

A third measure concerns the ban on spam, which goes back to the first version of the 1997 Directive. Since many individuals do not normally take action against spammers (either because they cannot afford to file a lawsuit, or because the damage they suffer is too small to start a procedure), a collective instrument has been created: From now on it is possible for natural and legal persons who have a legitimate interest in fighting spam to take legal action against spammers. Providers of electronic communications who want to protect their legitimate business interests or the interests of their clients and consumer associations and trade unions, who represent the interests of people who have suffered spamming, can now contribute to a safer Internet! In addition, the new directive also allows Member States to issue specific sanctions targeted at providers of electronic communications who contribute to spamming through negligence.

Finally (and fourthly), the 2009 Directive focuses on strengthening certain enforcement mechanisms. National data protection authorities should be empowered to prohibit further actions by persons or firms breaching the provisions of the Directive (prohibition order).

All three building blocks, identified by the UN Rapporteur, come beautifully together in this reform package. The road to justice is facilitated by better notification of security breaches, by enabling public interest groups to initiate legal actions and by making prohibition orders possible. Towards ICT companies and other relevant stakeholders, one can observe a change in approach. Mere compliance is refined and translated into real accountability: There must be an active policy towards the government and citizens (notifications), a safe final product (free from cookies, spyware, malware, viruses and spam) and sanctions are possible against the negligent offering of internet services.

The above illustrates the way forward. Responsible legislatures should set up a system that prevents human rights violations. They can do this by distributing certain responsibilities to stakeholders in the field. Their performance needs to be closely monitored by governmental authorities and access to justice needs to be made possible by a range of practical steps of which we have given numerous examples in this piece. At the moment, the EU is involved in a review process of the general data protection directive of 1995 and similar outcomes are to be expected in the years to come.

16. GENERAL CONCLUSION

In this contribution we have discussed the concept of the system responsibility of the government in the information society. This responsibility for ‘the whole’ exists with regard to the protection of personal data, but it of course also exists with regard to many other human rights sensitive areas such as the fight against identity fraud and the protection of media pluralism. Exploring these domains needs to be the object of further scientific contributions.

The responsibility, that we have discussed, is moral (legislators should pick up signals coming from society and act upon them, not merely giving in to economic stakeholders) and legally enforceable in accordance with human rights standards, legislation and jurisprudence.
Positive human rights obligations bring with them the obligation that the state should actively act against violations by government officials and individuals and has to take positive steps to ensure the enjoyment of fundamental rights. This requires supervision, legislation and policy-making. Policy makers must rely on criminal law when they are confronted with serious crimes. Tightening unclear penal provisions, introducing new penal provisions and using police and the judiciary cannot be ruled out. System responsibility often assumes distribution of responsibility. As has been done in the area of telecommunications, the relevant actors in society must be forced to take their share of responsibility and to respect the human rights expectations of citizens, notwithstanding proportional constraints. If this distribution is unbalanced or there is no distribution at all, then the government is ultimately responsible to the European Court in Strasbourg.

The assumption that European human rights law furnishes our governments with too few practical guidelines is unwarranted. In the area of data protection, the Court has developed general principles, which are applicable in more and more cases. To a lesser extent the same is true in the fight against identity fraud and the protection of media pluralism. Member states can put these principles to work and start evaluating the adequacy of existing remedies and compensation systems. The relevance of I. v. Finland (judgment of July 17, 2008) for the discussion of the establishment of the information society has not received sufficient attention. The judgment of the European Court of Human Rights states explicitly that the mere fact that national legislation allows for compensation is inadequate, and that there is a need for a practical and effective protection of personal data through legislation and enforcement. Providing a system of compensation based on fair and accessible conventional procedures is important, but insufficient. A full human rights abiding structure that both protects and develops (better: encourages development) is required and this operation is increasingly urgent. The information society has been around since the nineties and governments have already had the time to act appropriately.

This contribution began with a comparison between two debates, the first on the information society and the second on respect for human rights by multinationals in ‘weak’ countries. In both debates, there is a strong undercurrent against regulation and government intervention, and governance gaps are being covered up, created or supported, either in the name of the newness of the technology or in the name of the need for economic development in poor countries. 118

Within the responsibility paradigm several choices exist. Ruggie’s Protect, Respect, Remedy scheme indicates well the indispensable basic building blocks. Whenever the theme of accountability is addressed, all three blocks have to be considered for the sake of an integrative approach. The author of this contribution has not been able to temper his fascination for the third building block, the classical legal idea of remedy. However classical it may be, its relevance remains high. Too many public and private initiatives are launched and regulated from only one perspective, the perspective of the organism that takes the initiative. Seldom are initiatives looked at from ‘the back end’, from the perspective of the citizen that needs to be informed about his rights and from the perspective of the supervisory authority (judge or administrative authority) that needs to safeguard the fundamental right to an effective remedy. With Ruggie’s threefold scheme and his insistence on ‘real’ access to justice and real transparency the above trap is avoided.

Public authority has an important role to play in every integrative approach to accountability. It is up to governments to develop an efficient remedy system. Post-legislative scrutiny of key legal instruments adopted in the past should become the norm. A 2009 House of Lords’ report with regard to surveil-
Annex

...contains several recommendations for specific actions by governments that can be repeated here by way of illustration. Some of the questions that need to be addressed are the following: Do these instruments contain clear guidance on necessity and proportionality? Is priority given to citizen-oriented considerations? Can the safeguards and restrictions placed on surveillance and data handling be improved? Are design solutions incorporated? Can the introduction of a system of judicial oversight for surveillance carried out by public authorities be foreseen? Are individuals who have been made the subject of surveillance to be informed of that surveillance, when completed, where no investigation might be prejudiced as a result? Is compensation available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers?

Partly, these recommendations can be grouped together with state obligations to protect through effective regulations and effective enforcement (building block). Again a task for public authorities. In the ‘Evidence’ gathered by the House of Lords for its report on surveillance, that massive violations of security and privacy were not followed by appropriate sanctions was deplored: “When banks dump personal data in outdoor rubbish bins, in direct contravention of the Act, their punishment is to sign a form saying they won’t do it again. When the identities of staff at Network Rail and the Department of Work and Pensions are stolen from a compromised HMRC portal to defraud the tax credit scheme, HMRC escapes unpunished”. Improving the legal framework with regard to cybercrime, review of the data protection directive and more effective enforcement of privacy rules are rightly on the EU agenda.

With regard to the second building block (‘respect’), some favour a more stringent approach turning a duty to comply into a more active duty to prove that one is concerned and contributes to the protection of certain rights. The development should be applauded from a human rights perspective. Those who have power have to be held accountable. An information society that works, allowing providers, who do not see problems in unsafe and unregulated information services, is becoming less defensible. Citizens cannot be held responsible for a system where the government is not playing its role and forgets or refuses to hold relevant actors accountable. That is not how system responsibility works. The author of this contribution is aware of attempts to ‘sell’ more accountability in exchange of fewer formalities and less stringent data protection requirements on other fronts. From such a perspective, ‘more accountability’ seems to be instrumental for a kind of politics of good intentions (‘something went wrong but I am not responsible since I actively embraced data protection’). We recall that our legal system seldom considers good intentions and motifs, but does look at behaviour and consequences. Ethically it is important to embrace the active incorporation of human rights values, but legally there would be a flaw in system responsibility if no governmental reaction followed from damage caused.

ENDNOTES

1 Thanks to Dara Hallinan for many comments on earlier versions.

2 Although a lot of current attention focuses on the need to reform EU law, in particular data protection law, and on the need to enhance the duties of data processors to put data protection principles in practice, our paper ends with a long discussion on remedy and swift and accessible legal procedures, a building block that is often neglected in current discussions. We underline however that ‘system responsibility’ and comprehensive accountability implies that all three parts are equally important.

3 See www.dataprotectionday.eu.
Clearly, many think the question is not as simple, since the “open question of final responsibility” keeps returning in public discussions (luckily the answers are not always put to the vote). Even from a human rights perspective the argument can be made that this issue is not simple – particularly with the uncertainty as to the application of norms onto data environments. However the complexity can be reduced by taking European human rights case law as guiding principles as will be done below.


This Commission has now been replaced by the Human Rights Council.


It is important to realize the difference in composition of the Sub Commission, which is comprised of 26 independent experts, and the Human Rights Commission in which 53 government representatives take part. This particular composition shows the extended political character of the Human Rights Commission, in contrast to the Sub-Commission. This factor could be one of the underlying reasons for the ‘failing’ of the Norms.


For instance the British National Contact Point of the Organisation for Economic Cooperation and Development (OECD) makes us aware of the concept of due diligence of the SRSG in a human rights complaint against a corporation. In addition the International Organization of Employers (IOE), the International Chamber of Commerce (ICC) and the Business and Industry Advisory Committee (BIAC), amongst oth-
ers, accept the policy framework as guidance. Finally also non-governmental organizations (NGO’s), such as Amnesty International also recognise the importance of Ruggie’s work.


16 See, Art. 12 - 15 of Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000, concerning certain legal aspects of the services of the information society, more specifically electronic commerce in the internal market, Official Journal, L 178/1 of 17 July 2000. The directive is very lenient toward intermediaries, particularly with regard to the existing rules on criminal and civil liability in different countries. This directive aims to guarantee the free movement of information society services between Member States without internal borders. More freedom and confidence in electronic commerce is key. The text provides a horizontal (which is the same for all jurisdictions) limitation of liability for ISPs. It concerns Articles 12 to 14, which safeguard the service provider from liability for information on websites, which becomes available via its access service; when they are just a hatch (mere conduit), when they only stores those pages briefly when it is about frequently sought information (caching) or when they temporarily holds information about another (hosting). See critically, A. Lucas, ‘La responsabilité civile des acteurs de L’internet’, Auteur&Media, 2001, n°. 1, pp. 42-52.

17 Compliance means (only) that an organisation meets the rules, which are imposed from the outside or the inside. These are seen as a burden, which is borne grudgingly, but not as a trigger to create an asset-driven policy, whereby processes are adjusted. Accountability as proven trust needs to be contrasted with compliance as blind trust. In a scheme of accountability it is possible for the person involved to prove good behaviour because he or she took active, assignable steps to achieve a certain ‘good.’ See for a broader definition (over-broad) of compliance: De Vries H. & W. Janssen, ‘Compliance als kans’, Ego. Magazine voor informatiemanagement, 2010, vol. 9, n°. 3, pp. 11-15.


19 Idem.

20 All the judgments of the Courts are available via http://www.echr.coe.int/echr.

21 Only states can be judged in Strasbourg for alleged violations of the treaty. Complaints against corporations and individuals are inadmissible. Those have to be taken to national courts, but this presupposes that there is a judge, a sound legal system and a system based on human rights legislation.


27 In the *Stjerna* case the Court explains in an unusually clear way the difference between positive and negative obligations. The refusal of the Finnish government to allow Stjerna to change his name did not constitute an interference with his fundamental right to private and family life and the theory of the positive obligations should therefore be applied. It would be interference, according to the Court, if the government would force Stjerna to change his name (ECtHR, *Stjerna v. Finland*, judgment of 25 November 1994, § 38). About this aspect of the judgment: Lawson 1995: 743-746.


32 Op. cit. note 20, pp. 36-48, for a full description of these cases, their relevance and the application of the doctrine of positive obligations in relation to the protection of private and family life.

33 ECtHR, *Botta v. Italy*, judgment of 24 February 1998, § 34.

34 We can conclude, based on the previous decisions, that a violation of the rights contained in Article 8 ECHR is possible: - when the state interferes in these rights – when an abstention or a non-action on the part of the state ignores the rights recognised in the provision - when abstention on the part of the state gives the opportunity to third parties to ignore the discussed rights. See G. Cohen-Jonathan, *La Convention européenne des droits de l’homme*, Paris, Economica, 1989, p. 375

35 Moreover, it is necessary to specifically examine whether there is a link between a possible positive obligation and the complaint of the subject which invoked the allegation of violation of fundamental rights.

36 ‘The Court does not consider that Ireland can be said to have “interfered” with Airey’s private or family life: the substance of her complaint is not that the State has acted but that it has failed to act. However, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition
to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for family life (see the above-mentioned Marckx judgment)” (ECtHR, *Johanna Airey v. Ireland*, judgment of 9 October 1979, § 32).


38 ECtHR, *X and Y v. The Netherlands*, judgment of 26 March 1985. One day after her sixteenth birthday, Y was sexually abused by the son of the director of the residence for the mentally handicapped, where she stayed. After a decision not to prosecute by the public office, her father (X) went to court claiming that a crime had been committed; ‘deliberate inducement of minors to sexual abuse’ (Art. 248ter Dutch Criminal Code). The Arnhem Court declared the case inadmissible because, pursuant to the Criminal Code only the victim may lodge a complaint and for people under sixteen, legal representation is provided. In Strasbourg, father and daughter claimed that there had been a violation of Article 8, 3, 13 and 14 ECHR. With regard to Article 8 ECHR, they argued that for a young girl such as Y, only criminal protection is sufficient and that states have a positive duty to create sufficient legal protection through criminal law.

39 ECtHR, *X and Y v. The Netherlands*, § 23. The ‘effective respect’ for private life implies, the Court held, that the state has a positive obligation to take measures to ensure privacy, even in the sphere of relations between individuals.

40 ECtHR, *X and Y v. The Netherlands*, § 27. The right to respect for private life requires member states to take measures in criminal law to protect sexual integrity. There is a margin of appreciation left to states regarding their policy to combat sex crimes and aggression, but as in this case, a civil law protection does not satisfy and is simply not enough. Additional criminal law protection is needed for serious violations of sexual integrity.

41 Renchon, l.c., pp. 98-102.


43 See ECtHR, *X and Y v. The Netherlands*, § 23.


45 The facts did not lead to the punishment of the offender due to certain legal difficulties. Because the alleged victim could not prove that she resisted the sexual acts, the accused were not criminally convicted. The applicant stated that in the summer of 1995, when she was fourteen years old, two men raped her. She volunteered to go along with three vague acquaintances in a car to a disco, but the men then took her to a pond, allegedly for swimming. The first rape happened there. Frightened and embarrassed the girl had not the strength to resist. Subsequently she went with the men, back to a house where a second man raped her. In his own words, she cried and begged to stop, but offered no physical resistance. When her mother found her the next morning in that house, she brought her to the hospital where it was found that she had had sexual intercourse. The men did not deny this, but claimed that the intercourse was voluntary. Eventually it ended in a lawsuit, whereby the men were acquitted. The judge found no evidence that the girl was violently forced to have sex, since there was no evidence that she resisted.

46 The Court reproached that the Bulgarian courts, in the absence of direct evidence of rape, did not reconstruct the circumstances of the crime and did not evaluate the credibility of the contradictory statements
from which possible indirect evidence of absence of consent could be inferred. The report of the Bulgarian researchers showed that the Bulgarian judges did not rule out that the girl did not consent, but that they, because of lack of evidence of resistance, did not want to conclude that the perpetrators had understood that she did not consent. The Court stated explicitly that in rape cases there is an obligation to focus the investigation on the question of consent, and from that perspective to investigate all the relevant facts and circumstances. It should also take into account the special vulnerability and specific psychology of young victims. According to the Strasbourg judges, the Bulgarian government failed to fulfil the public duty to offer effective criminal law protection against rape and sexual abuse. Consequently, the Court concluded that Articles 3 (right to protection against inhuman treatment) and 8 (right to privacy) ECHR were violated.

47 In Bulgarian law, rape is only punishable when there is evidence of resistance by the victim. Simply not agreeing is insufficient. The text of the Bulgarian criminal provision on rape requires no evidence of physical resistance, but the requirement is ‘read into’ the provisions by the courts. For the European Court this state of affairs does not meet the European standards requiring states to criminalise and effectively prosecute non-consensual sexual acts, even if the victim did not physically resist. The Court bases this interpretation, amongst others, on the evolution of criminal law in this area in most European countries, as well as on the law of the International Criminal Tribunal for former Yugoslavia. In particular, Article 8 ECHR provides for measures to regulate relations between individuals. Particularly severe violations of fundamental values and privacy cannot be settled by legal protection, which is not based on criminal law. In this context criminal law is the only appropriate government measure. See paragraph 150: “Positive obligations on the State are inherent, in the right to effective respect for private life under Article 8; these obligations may involve the adoption of measures even in the sphere of the relations of individuals between themselves. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is in principle within the State’s margin of appreciation, effective deterrence against grave acts such as rape, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions. Children and other vulnerable individuals, in particular, are entitled to effective protection.” (see ECtHR, X and Y v. the Netherlands, judgment of 26 March 1985). In combination with the investigation and enforcement duties based on article 3 ECHR, the Court decided that: “States have a positive obligation inherent in Articles 3 and 8 of the Convention to enact criminal law provisions effectively punishing rape and to apply them in practice through effective investigation and prosecution” (ECtHR, M.C. v. Bulgaria, § 153.)

48 Of course, when there is no human rights problem or conflict, then no positive state duties come into play. If one were to imagine that the information society was human rights neutral, then nothing would need to be done. The well known popular mantras about self-regulation by industry could then be made heard.

49 Additional evidence for this statement will be given with the discussion of judgments such as Gaskin, Peck and I. v. Finland below.

50 If it does not turn ICT firms into policemen, it will have to police them individually.

51 A. Meijer, l.c., p.101 and following.

52 Idem, p. 111 and following.

53 Idem, p. 98 and 106.

54 Meijer, a non-legal scholar that has guided us considerably with his work on responsibility, seemingly downplays the legal dimension of this broader notion of responsibility.
In Strasbourg’s human rights perspective, the government is made responsible for not responding appropriately to human rights violations under its jurisdiction. Strasbourg, therefore, takes care of the legal leap from responsibility for its own disputes to ‘system responsibility’.


This contribution by no means wants to open the globalization discussion. It however strikes us that authors such as Tully and Kreide, both elaborating constructive proposals to strengthen the legitimacy of contemporary norm setting procedures, highlight political legitimacy and participation, but ignore ‘simple’ legal responses, such as the Strasbourg system discussed here, which strengthen rule of law legitimacy. See J. Tully, l.c., pp. 204–228 and Regina Kreide, ‘The Ambivalence of Juridification. On Legitimate Governance in the International Context’, Global Justice: Theory Practice Rhetoric, 2009, Issue 2.

Much of what is involved in legal protection, is the unravelling of decision-making processes, to determine whether the process of the practice has been meticulous in all phases. Such process is much more difficult to verify when automated processes are involved, because then, how the system was designed must be tested. This can be a rather difficult, abstract, and meaningless exercise.

Again we remind the reader that additional evidence for this statement will be given with the discussion of judgments Gaskin, Peck and especially l. v. Finland below.


More than often judges restrain themselves because of the scarcity of societal resources. If a judge accepts a claim, it will often be at the expense of other necessary government functions (O. De Schutter, l.c., pp. 42-43). De Schutter refers to the work of Lon Fuller who developed the idea of poly-centrality: certain disputes are inherently incapable to be judged by courts because they hide complex issues and interests that are interlinked. See L Fuller, ‘The Forms and Limits of Adjudication’, Harvard L Rev, 1972, Vol. 92, p. 353 and further.

This is consistent with the view that the European human rights system is based on the so-called subsidiary principle. This principle states that the protection of the rights enshrined in the Convention is primarily a matter for the member states. They should ensure an effective protection and redress possibility when protection somehow fails. The European system only plays a complementary role and will only be visible when the national authorities do not, or insufficiently, devote themselves to their duties. Cf. J. Vande Lanotte & Y. Haeck, Handboek EVRM: Deel I Algemene beginselen, Antwerp, Intersentia, 2005, pp. 179-180. The principle is not explicitly reflected in the European Convention on Human Rights, but rather inherently present.

Compare with ECtHR, Armonas v. Lithuania, judgment of 25 November 200 § 46: “The Court agrees with the Government that a State enjoys a certain margin of appreciation in deciding what ‘respect’ for private life requires in particular circumstances (see Stubbings and Others v. the United Kingdom,
judgment of 22 October 1996, §§ 62-63; ECtHR, X and Y v. the Netherlands, § 24). The Court also acknowledges that certain financial standards based on the economic situation of the State are to be taken into account when determining the measures required for the better implementation of the foregoing obligation.”

65 ECtHR, Armonas v. Lithuania, § 38: “The Court reiterates that, as regards such positive obligations, the notion of respect is not clear-cut. In view of the diversity of the practices followed and the situations obtaining in the Contracting States, the notion’s requirements will vary considerably from case to case. Accordingly, this is an area in which the Contracting Parties enjoy a wide margin of appreciation in determining the steps to be taken to ensure compliance with the Convention, account being taken of the needs and resources of the community and of individuals (see ECtHR, Johnston and Others v. Ireland, judgment of 18 December 1986, § 55). The Court nonetheless recalls that Article 8, like any other provision of the Convention or its Protocols, must be interpreted in such a way as to guarantee not rights that are theoretical or illusory but rights that are practical and effective (see Shevanova v. Latvia, judgment of 15 June 2006, § 69).”

66 A citizen or group cannot go to Strasbourg as a result of absence of a legal regime for technology when there is no identifiable, concrete human rights problem. This is what happened when the Belgian League for Human Rights went to Strasbourg to challenge the lack of specific regulation concerning CCTV in Belgian legislation. The complaint was declared inadmissible. See European Commission on Human Rights, Pierre Herbecq and Ligue des droits de l’homme v. Belgium, Decision of 14 January 1998, requests n°. 32200/96 & 32201/96, J.T.D.E., 1998, pp. 67-68.


68 The British government had unsuccessfully invoked Article 10 ECHR. The defence was that an effective legal protection against the violation of the right to privacy by the media was a threat to press freedom. The Court, however, does not agree. The Court considers that “the Council, and therefore the media, could have achieved their objectives by properly masking, or taking appropriate steps to ensure such masking of the applicant’s identity”.


70 Between 1989 and 1994 the applicant worked as a nurse on the eye diseases ward in a public hospital in Finland. Since 1987 she had regularly visited the ‘contagious diseases’ department in the same hospital as she had been diagnosed with HIV. After working for three years in the hospital she started to suspect that her colleagues knew about her illness. At that time employees of the hospital had free access to information on patients and their health. At her request, this situation was put right by only allowing the staff members responsible to have access to their patients’ records. Further, the claimant was registered under a false name and under a new unique number. In 1995, however, her contract was not renewed. In November 1996, the claimant complained to the County Administrative Board about misuse of her personal data. She asked to be allowed to see who was able to access her information. The responsible official claimed that this was impossible claiming that the system only showed the five most recent consultations and the consulting department, not the person who had consulted the file. In addition, this information had been removed when the file was put back in the archive. The complaint of the claimant was therefore dismissed. Afterwards, the archive of the hospital was adjusted in such a way that it became possible to identify the person who had consulted the patient data. A series of civil proceedings, which were brought before the District Court and Court of Appeal by the claimant against
the authority which was responsible for monitoring the hospital, were all rejected because the claimant could not prove that her data had been consulted illegally. An appeal to the Finnish Supreme Court was also rejected, whereupon the claimant brought the claim to the European Court of Human Rights. In Strasbourg the claimant argued that the Finnish Supervisory Authority had failed in its obligation to set up a system in which patient records could not be used illegally, which she considered to be contrary to Article 8 of the ECHR. According to the claimant the requirement for retrospective monitoring is essential to respect this right. The Finnish government replied that the national legislation adequately protects patient data and that “systems which are developed in hospitals that make the record keeping of patients possible, can only work properly if detailed instructions are given to staff, when they respect high moral standards, when there is supervision and when the staff respect professional secrecy.” In this case, it would not have been possible, according to the Finnish government, for the hospital to create a system whereby the authenticity of every request could be controlled in advance, since access to the data was often required immediately and urgently.

71 ECtHR, I. v. Finland, § 36.

72 ECtHR, I. v. Finland, § 38.

73 ECtHR, I. v. Finland, § 38.

74 ECtHR, I. v. Finland, § 40.

75 ECtHR, I. v. Finland, § 47.


77 In this regard, she does not only complain about a breach of Article 8 ECHR, but also of Article 6 and 13 ECHR.

78 ECtHR, I. v. Finland, § 44: “The Court notes that the applicant lost her civil action because she was unable to prove, on the facts, a causal connection between the deficiencies in the access security rules and the dissemination of information about her medical condition. However, to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital’s record keeping at the material time. It is plain that had the hospital provided greater control over access to health records by restricting access to health professionals directly involved in the applicant’s treatment or by maintaining a log of all persons who had accessed the applicant’s medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts. For the Court, what is decisive is that the records system in place in the hospital was clearly not in accordance with the legal requirements contained in section 26 of the Personal Files Act, a fact that was not given due weight by the domestic courts.”

79 “The Court finds it established that the applicant must have suffered non-pecuniary damage as a result of the State’s failure to adequately secure her patient record against the risk of unauthorised access. It considers that sufficient just satisfaction would not be provided solely by the finding of a violation and that compensation has thus to be awarded. Deciding on an equitable basis, it awards the applicant EUR 8,000 under this head” (ECtHR, I. v. Finland, § 47).

There is insufficient evidence for the extramarital relationship so that triggers compensation, the local court held, but there was no reason to give compensation for the other facts: the information on the extramarital relationship and health status were not made known intentionally.

It was not clear whether further action was possible for the family of the original victim of a possible violation of a treaty right. The Court responded positively about this. The Court finds that the claimant may apply to the European Court as a victim. The Court had previously held that a case would be inadmissible if it were to declare the substance of the matter too closely linked to the deceased and untransferable to the heirs. However in this case this was not the case. Following the publication of the article the family was forced to move and also the national courts had ruled that the article had limited the communication ability of the family. The article therefore had a negative impact on both the applicant and her child. The argument of the Lithuanian government that the applicant was not a victim anymore, because the national judge had already ruled a violation of her private life and compensation had been awarded, was dismissed. This does not affect a possible classification as victim “Where Does The Quote Start Here?.

To better balance both rights at stake, the Court distinguished, with regard to the freedom of the press, between distributing factual information as part of a public debate on the one hand, and distasteful allegations concerning the private life of a person on the other (ECtHR, Armonas v. Lithuania, § 39). Turning to the right to protection of privacy, the Court observes that the right is there to encourage people in their development. The protection offered goes far beyond the family circle and includes a certain social dimension of individual privacy (ECtHR, Armonas v. Lithuania, § 39). Privacy as a fundamental right was therefore found to be undoubtedly applicable to this case.

The main findings of Armonas about the protection of persons in the media were already present in another famous case, this time from the Court of Justice in Luxembourg: Case Bodil Lindqvist on 6 November 2003. However Armonas enlightens us further than Lindqvist about how to make the balance between the protection of privacy and protection of press freedom and expression, especially through the important distinction between the distribution of factual information as part of a public debate on the one hand, and distasteful allegations concerning the private life of a person on the other. See Court of Justice, Bodil Lindqvist, case C-101/01, judgment of 6 November 2003 via http://eur-lex.europa.eu. In this judgment the Court of Justice judged the electronic publication of personal data on a website on the Internet in the context of Directive 95/46/EG concerning the data protection of natural persons. The case concerned a volunteer in a protestant church community in Sweden, who on their own initiative had developed web page and had disseminated names, telephone numbers and information about their proceedings and hobbies, not just about her but also about her colleagues. In addition, she mentioned that one of her colleagues had injured her foot and was on sick leave.

90 See in addition to Armonis also ECtHR, Reklos & Davourlis v. Greece, judgment of 15 January 2009,§ 47.


94 About the lack of purpose limitation principle in the law of the United States, see De Hert and Bellanova 2008.

95 V. Pop, ‘Ripples of discontent as MEPs reject US bank data deal’, EUobserver, 2010 via http://euobserver.com/9/29455/?rk=1


See L.C. Baldor, ‘Experts say US must do more to secure the Internet’, *The Associated Press*, February 23, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/23/AR2010022304211.html. “Comparing the digital age to the dawn of automobiles, analysts said more government regulations may be the only way to force the public and private sectors to adequately counter cyber threats. They compared the need for new oversight to regulations for seat belts and safety equipment that made the highways safer.”


ISDN stands for Integrated Services Digital Network.

Art. 5 Directive 97/66/EC.

Art. 8 Directive 97/66/EC. The directive gives each subscriber the possibility of free per-call caller ID blocking (with the possibility to turn it off), so he remains anonymous. Also, each subscriber has the ability to block certain incoming numbers. In some cases calls may unblocked: for example with heavy breathing calls, as part of a criminal investigation and calls relating to certain emergency services (art. 9 of Directive 97/66/ EC).

Art. 6 Directive 97/66/EC. Some data are allowed to be stored and sold, but in that case the subscriber has the right to resist, in the sense that he must agree to the sale.

Art. 3 Directive 97/66/EC.


The ePrivacy Directive is a specific directive and the new measures focus primarily on the providers of electronic communications such as telecommunications companies and Internet service providers. Given the growing interdependence between the I (information) and C (communication) from ICT this is already a substantial group within the information society. There is also the expectation that a number of new measures from the ePrivacy directive will be generalised in the forthcoming review of the general directive of 1995, so they will apply to everyone processing personal data, including those outside the telecommunications sector.

An “infringement in relation to personal data” is broadly defined as “a breach of security leading to the accidental or unlawful destruction, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications in the Community”.

In its notification to the user, the provider has to at least state the nature of the infringement, the relevant contact information and suggest measures to alleviate the potential negative consequences of the violation. The individual user does not need to be notified if the provider shows to the competent national authority that he has protected the information with technical protection measures that make the data unintelligible to unauthorized parties. If the provider decides not to inform individual users but the national competent authority considers that the infringement may have an adverse effect on individual users, it can force the provider to inform individual users. This authority may also issue instructions on the circumstances in which notification is required, their format and how the notification should be done.

Some of the imperfections of the 2002 ePrivacy Directive have been eliminated in the new regime. Amongst others, the scope of the ban is extended. Under the old system this was limited to the situation where the access and information storage on the user devices was done through electronic communications. It was not clear whether the scheme was applicable to the situation where cookies, spyware and the like ended up on the user device through software ended up on external storage media (such as CD-ROMs and USB sticks) or downloads. To ensure that these would also fall within the scope, the words “through the use of electronic communications” were deleted.


See the declaration of State Secretary of Economic Affairs in his letter to the Chairman of the House of Representatives, 30 May 2008, the House of Representatives, Conference year 2007–2008, 31200 xiii, nr. 57.


I INTRODUCTION: THINKING GLOBALLY

International agreements, ‘European’ standards

International agreements concerning data privacy have contributed a great deal to the development of consistency of national data privacy laws. From the start of the 1980s the non-binding OECD privacy Guidelines (OECD, 1980) and the first binding international agreement, the Council of Europe data protection Convention (CoE, 1981 - the Convention for the protection of individuals with regard to automatic processing of personal data), both embodied privacy principles with many similarities but not identical substance, and expressed in somewhat different language.

From the mid-1990s the European Union’s data protection Directive (EU, 1995) embodied a set of privacy principles consistent with, but somewhat stronger than, those in the OECD and CoE agreements. However, the Directive added much stronger enforcement requirements, including establishment of an independent DPA and a right to have disputes heard by the courts. Unlike either of the earlier agreements, it also required limitations on data exports to countries outside the EU which did not have ‘adequate’ privacy laws (discussed in more detail later). The standards set by the Directive have become recognised as the strongest standard for data privacy in an international instrument. The Convention also now has an Additional Protocol (ETS No 181 – CoE, 2001) requiring data export limitations and supervisory authorities, so as to better align it with the Directive.

This paper considers the implications of these two key European privacy standards – Council of Europe Convention 108 (and its Additional Protocol) and the EU Directive – for countries outside Europe. But their implications for European countries are also changing.

The real world of data privacy laws: 78 countries and growing

In ‘Global data privacy laws: Forty years of acceleration’ (Greenleaf, 2011) the question ‘How many countries now have data protection laws?’ was answered with ‘76’, but the answer is now ‘78’ since Costa Rica adopted a data privacy law in September 2011, and Vietnam’s new consumer protection law (containing a privacy code) came into effect in July 2011. The unexpectedly high answer (the conventional answer was a somewhat vague ‘about sixty’ or perhaps ‘more than sixty’) has considerable implications for European privacy standards.