The portrait[1] – Privacy icons – Peter Hustinx

‘Occasionally you do have to bang the table’

Jeroen Terstegge and Koen Versmissen

In January Peter Hustinx’s second term as European Data Protection Supervisor (EDPS) came to an end. In the meantime it has become known that he will remain in this post until 16 October this year so that the Commission has sufficient time to find a successor. With his approaching retirement in sight, it is a good time for us to look back at Peter’s impressive career in the field of the protection of personal data.

How did privacy become your area of expertise?

That’s a long story, but you can split it into two parts. There was a period of almost twenty years when it was among the subjects that kept me occupied and after that the period with the Registratiekamer [Dutch Data Protection Board], the CBP [Dutch Data Protection Authority] and the EDPS where I was working on it full-time. Initially it was a chance consequence of my studies in the United States, where, among other things, I came into contact with the very early thinking about privacy. In 1967 Alan Westin had already written a book (Privacy and Freedom, ed.). But between 1970 and 1971 I studied with Arthur Miller, the lawyer who had written the book The Assault on Privacy (1971) and who held a workshop on the subject. I found it interesting. Then, when I came to the Ministry of Justice in 1971, there had just been two major upheavals in this area: one was the census (1971, ed.) and the other was the fuss surrounding the CPA number (CPA=Central Register of Persons, ed.). The Biesheuvel government at the time had therefore included in its coalition agreement that they were going to do something about privacy, and they set up the Koopmans Commission in order to do so, of which I then became assistant secretary. As a result of this I not only nosed around the first outlines of privacy legislation at an early stage but also participated at the same time in what was happening at the Council of Europe in this area (Convention 108, *ed.*).

Then, at the end of the 1980s, when work on the Data Protection Act was completed, I worked in the ministry mainly on criminal law, criminal procedure law and administrative law. But two years later, when the first chairman of the Dutch Data Protection Board, Klaas de Vries, stood down, I was put forward. I asked myself at that point whether I really wanted to do this after twenty years but, in the meantime, it had become clear to me that this subject had far-reaching consequences and potential and that it was exciting to play a role in it. It was also true that in the beginning it was not only about the principles, or even the content of the law, but very soon also about the question of which means needed to be employed to enable it to work. Should that be through civil law, criminal law or administrative law? And what institutions do you need for that? The Koopmans Commission advocated setting up a kind of Chamber of Information. Owing to the wave of deregulation in those years I found it fascinating to think about a Chamber which was not only effective but which also needed not to cost too much. Furthermore, it involved a wide range of work: not

[1] This interview appeared in ‘Privacy & Compliance’, *Tijdschift voor de praktijk*, 01/2014, pages 4-13.

only justice, but also healthcare, telecommunications, transport, social security and the population registers.

On 1 July 1991 I became Chair of the Dutch Data Protection Board. That coincided with the Dutch Presidency of the Council, and then the draft of Directive 95/46 was on the table in Brussels. The European Commission had proposed a Directive with a very German stamp, with a clear distinction between the private and the public sector. Under the Dutch Presidency it was then decided to integrate it into a single set of rulesn. I was very closely involved in the discussion and then fell fairly naturally into the role of Chair of the Article 29 Working Party. After this the Chairmanship of the CBP [the Data Protection Authority] and my appointment to the EDPS followed.

You have also been closely involved in European policy-making.

In the European context it was mainly the Council of Europe which played an important role, which approached this subject from a human rights perspective. They were mainly concerned with the creation of law, not the economy or technical matters, though they did wonder how technology might impact on human rights. At the time people already thought that technology would have a very far-reaching impact. It was assumed that the issue of protecting personal data would lie somewhere between privacy and freedom of information. But there was nothing about this on paper. People therefore wanted to know what the principles of the proper use of computers would actually be. And even before Convention 108, that led to a couple of recommendations. The first was about the private sector. It was fairly easy to get those principles down on paper. Then there was also a recommendation for the public sector, but with some special arrangements because of the particular position of government authorities, such as the police. These two recommendations were the basis of Convention 108. That convention obliged the Member States to transpose it into national law. The European Commission was then worried because of the diversity which arose from it. We devoted the first two years of the negotiations about the Convention to creating its main structure. The rest of the time was devoted to the arrangements for transferring personal data (Article 12), the applicable law and national jurisdiction. And those last two items did not make it into the Convention in any case because at the time they were still far too complicated. And they still are for that matter.

When the Convention was finished, the question arose as to what the general principles would now mean exactly in specific areas. Therefore, a number of corrections were also made to the convention, such as the concept of ‘personal data’. Initially the wording was ‘easily identifiable’, but that was changed to a more neutral definition. The principle of purpose limitation was there already at a very early stage. That was also a logical consequence of the thinking in the European Convention on Human Rights. Every infringement of a fundamental right is linked to a purpose, measure and legal foundation. The step which the law on data protection made was that there always had to be a legal foundation for the processing of personal data, irrespective of the question of whether an infringement of a fundamental right was involved. Therefore, I also find that privacy and data protection are essentially two completely different things, although they do overlap. The curious thing is that the consequence that that has not only for collecting and storing data but also for using it – the incompatibility concept – only became apparent at a very late stage. But then

immediately doubts arose: only the same aim, is that not a little too strict? This term ‘incompatible’ was already to some extent part of human rights case-law, and the Instructions for the Civil Service, which involved a form of self-regulation even before the WPR [the Data Protection Act], also recognised the principle of incompatibility. You can therefore best compare the development of the principles of data protection with a Wiki process; throughout Europe people were working together to arrive at wordings through an iterative process.

The OECD principles have survived the ravages of time reasonably well. But under the influence of developments such as Big Data they are increasingly called into question.

Of course I recognise the challenges, but I am also struck by the great continuity. Nothing is set in stone, that would also be unjustified. But since 1980 about every ten years there has been an assessment which has revealed that the principles are still valid. Furthermore, as regards content, the OECD principles are similar to those of the Council of Europe. When the European Union started its review, the OECD and the Council of Europe also decided to review their guidelines or convention. The OECD review was completed in June 2013. But if you look at it more closely, it is really just a confirmation of the old guidelines. Only accountability receives far more emphasis and there is more discussion about international cooperation. The conclusions are therefore clearly based on a common understanding. If, for example, you look at what President Obama says about privacy in the private sector, he essentially arrives at the same principles. The Americans call that *reinvigorated FIPS* (Fair Information Principles, *ed.*), but in essence it comes down to the same thing. But I think that you always have to see the OECD principles in a context and that context has changed enormously in the past few years. For example, in some cultures, such as Germany and Austria, consent is over-emphasised. On the other hand, there are also countries which do consider consent to be important but where the conditions for it are very flexible in practice. That way you undermine the system.

For example, a few years ago the European Court rapped Spain over the knuckles for the unreasonable limiting of the legitimate interest in marketing. The drawback of the Spanish approach was that, on the internet, you see many instances of consent being obtained easily, or even abuse of consent. People are happy to take consent as grounds for legitimacy, but prefer not to think about what happens when consent is refused or withdrawn. My advice is: if it is too onerous to ask for consent, then don’t do so. Consider the execution of a contract, complying with legal obligations or legitimate interest. In the latter case you also have to think much more about why you think that what you are doing is legitimate. The question then is: is my default position which I am putting to the data subject such a good offer? There is therefore a case for strengthening the grounds of legitimate interest with an external obligation of responsibility.

Within the framework of Directive 95/46 it is very clear that consent is only *one* reason for legitimacy, in addition therefore to others which all work in their own way. A balanced system should leave room for legitimate interest. In the Opinion on Purpose Limitation (WP 203 of the Article 29 Working Party, *ed.*) you can see these balances working. That report also discusses Big Data and Open Data. I would be the last to say that the application of privacy principles to those developments is

without problems but I do not agree with those who say that the principles are no longer fit for purpose. It does not help to make things clearer if you say that because of the great volume of data the only thing that matters now is the use of it. The use is the test and there protection must be very good but I think you always have to start from the perspective of obtaining the data. Good data management now begins with thinking about the collecting of data. If you don't do so you will never find good solutions. As far as I am concerned, the principles are still valid. With a few small adjustments they can simply be kept. But you must bear in mind the balances they entail. From that point of view, the distribution of responsibilities concerning the application of the principles is the core question of the discussion. I therefore see the revision of European law on data protection as a clarification of the principles, not least in order to ensure that they are implemented in a practical manner in the context in question.

How do you look back on your period as EDPS?

It was very much an experience of making something out of nothing. When I arrived there was nothing at all, not even a budget. The best part about it is that the EDPS is now an institution and does all kinds of things. The Regulation by which the EDPS was set up (45/2001, *ed.*) is a kind of European Data Protection Act. In it we saw strategic lines: 1) supervision, 2) legislative and policy advice, and 3) cooperation with fellow supervisory authorities. The first main task is to ensure that the Regulation is complied with by the European institutions. Initially there was the same resistance which you saw at national level (no priority, no staff, etc.) We used accountability as a mechanism to give space to the controllers, but to hold them to account. We also use benchmarking to show how institutions are doing compared with each other. And you can see that they have made real progress.

Improvements can always be made of course but in general most score quite highly. We also use benchmarking results to highlight underperforming. The institutions are singled out by name, and of course they don't like that. The underperformers receive special attention from us. We pay them a visit and a roadmap is drawn up for improvement, with monthly reports. As far as I am concerned this supervisory task is being carried out very well.

You have also acted decisively as to legislation in Europe.

I found legislative and policy advice strategically very important and I therefore encouraged it strongly. I didn't think I should wait but rather that I needed to join in actively with things which were taking place here in Brussels. That also had to do with my background. That therefore became our second main task. We have a methodology for this. Every year we analyse the Commission's agenda. We score it for relevance and we say roughly what we expect of it. And while the Commission is still thinking about the subject, we are prepared to give advice on it if the Commission asks us to do so. But if a proposal is adopted, they must present it to us and the advice becomes public. We started using this method when 9/11 was still a relatively recent event and privacy was certainly not a popular subject in the third pillar (police and judicial cooperation, *ed.*) at the time. Nevertheless, we offered these methods over the whole range of policy-making. And to my great satisfaction the Commission,

the Parliament and the Council have cooperated actively on this for all these years. Things could have been different.

You have also sometimes been very critical in certain areas.

Occasionally you do have to bang the table. Not too often, otherwise they think ‘there he goes again’. But over the years we have done so very emphatically about a dozen times and that’s worked well. The regulation also gives me the facility to intervene in disputes before the Court of Justice. According to lawyers that was a questionable provision. Really only the classical institutions may do so. But when the case concerning passenger name record data (PNR) came before the Court, I found that I had a historic opportunity to intervene. And the Court allowed me to do so. According to the Court, the EDPS was to promote compliance over the full range of the law. And of course I framed this. Since then advising has taken on a different dynamic. Our advice was taken more seriously, precisely because we could come back to the Court. That has been an incredibly fortunate coincidence.

And the third task?

That is cooperating with fellow supervisory authorities. This has grown gradually. Of course in the Article 29 Working Party I am by far the longest-standing member. If you introduce your points selectively, you will get a lot done. We introduced our positions on the most strategic subjects. For example, think of the key privacy principles and the BCRs [Binding Corporate Rules]. I think that that contributed to the Commission proposing that the EDPS be involved in the work of the European Data Protection Board (EDPB).

Are you satisfied with what you’ve achieved?

Yes, I am reasonably satisfied with what we, as the EDPS, have achieved. There have, of course also been things that I was less happy about. Take, for example, data retention. I advised against that but ultimately it went through nevertheless. But it is satisfying that with the Irish/Austrian referral, where we are not permitted to intervene, the Court asked us to come to argue the case. We now just have to wait and see what the Court does with our advice. Another highpoint in my opinion was that, after I had advised that amendment of Directive 95/46 was unavoidable, the Commission went ahead and did so, albeit with some moaning and groaning, and since then I carried on contributing to the revision.

What is the greatest challenge for your successor?

A number of things have not yet been finished. They of course include the revision of the European privacy framework. But there are also risks. Criticism also increases the more you put yourself in the spotlight. We are not a political institution but sometimes we have made our position clearly known. And then you must not be in the wrong place at the wrong time. That can turn out ugly. You need to be a good helmsman.

It is almost likely that your success as EDPS will make it difficult to find a good successor.

I can't be happy about that. The problem is currently before the Council and the Parliament. They decide whether the procedure will continue or will be closed. But ultimately they will find somebody who can take over the baton.

Every European institution must have at least one DPO. Do you work together with these DPOs?

Yes, we work a great deal with the DPOs. There is a meeting three times a year with all DPOs. Furthermore we work monthly, weekly or even daily together with DPOs, via email and telephone, for example. The DPO is put in copy on all matters. At an early stage we also positioned the DPOs as strategic partners for the controllers. For example, we inform the DPO of our activities well in advance. In this way we ensure the involvement of the DPO in the matters which concern him. And at the Commission for example, there are two DPOs, but also some thirty-five data protection coordinators, one in each DG. These 30-40 people, a number of whom are part-time, are the backbone of accountability in practice. We have kept the DPOs sufficiently at a distance to allow them to function as they see fit, and sufficiently close to support them where necessary.

The Regulation requires organisations to take all kinds of measures, including appointing a DPO. There are often no such specific requirements for other compliance subjects, and this sometimes gives rise to resistance in organisations. How does a DPO ensure that he or she is taken seriously?

I certainly recognise that. We have therefore drawn up a memorandum about the position of DPOs, including subjects such as the independent nature of the DPO, the DPO as a part-time function and who the DPO reports to (how high in the organisation?) Furthermore, the DPOs have developed a code of conduct endorsed by me, which states what a DPO has to do when he has just been appointed, what his priorities must be, etc. A DPO must ensure *buy in*. He must draw up a programme and seek support for it. That programme must be related to the mission of the organisation. The organisation must be able to understand how it will be better because of it. Of course some things are obligatory but a good privacy policy can also offer opportunities. A DPO must therefore not sit on his hands. Successful DPOs are those who take up that challenge. I also think that it is not true to say that there are no detailed provisions in other subjects. Look, for example, at the rules for bookkeeping and the rules for accountancy which have existed for many years. But you also see comparable rules in newer areas. Think, for example, about accounting for chemical substances and emissions. Detailed provisions also apply in the field of health and safety at work. In principle, the revision of the Directive follows the same thinking.

The point is to give compliance shape in practice. Responsibility is not a definition but an action. And then you arrive at accountability. The term itself does not appear in the Regulation but over the years business has studied all aspects of accountability in depth and then you come to the same conclusions: it is a question of *data management.* But I am only partly pleased with the way in which that is set out in the

Regulation. The Commission has coloured some parts in too old-fashioned a light, such as the determination of proof (the documentation requirement of Art. 28, *ed.*). Of course there is a need for proof, but it is not necessary that organisations have an accurate description of how they process things every minute of the day. We had that with the notification requirement. I have advised stipulating that there has to be a method for managing processing. That can then be standardised and specified further sector by sector. We are now working on a *risk-based approach* in order to ensure that these kinds of obligations can indeed work.

Old-fashioned enforcement obligations have rightly been cut out of the Regulation. The notification requirement for processing is an example of this. These have been replaced by newer ones, although the right scale has not always been used. The Commission would have done better to describe the characteristic elements of responsibility, such as adopting measures, examining their effectiveness and having evidence to be able to demonstrate this. And then it would have been able to describe what steps have to be taken at the minimum. The provisions as they now stand in the Regulation can be justified in a single cultural sphere, but it is certain that the final outcome will be very different in 28 different countries. It is therefore a challenge to produce uniform rules, which are then not too restrictive but are suitable everywhere. I believe that on that point we are, particularly in the Council, closer to the outcome than is generally assumed.

Moreover, in my opinion, the costs of the measures are grossly exaggerated. No account is taken of the benefits or of the costs of friction. Current non-compliance is also ignored. The Commission has stirred up feelings by threatening fines amounting to millions. These are of course scalable, but nevertheless form an extraordinarily effective means by which to draw attention in the *boardroom*. And then you need supervisors who deal with it in a sensible way. That means that they have to reward good practice and act firmly where it is wrong. Therefore supervisors not only have to have the authority to hand out fines but also to demand a plan of attack and progress reports, coupled with sanctions to spur on organisations. But you cannot do that for the whole economy. A supervisor must therefore be able to explain properly why he is acting in a particular case.

The digital economy is now wholly international. How do we adapt our European privacy values to the global playing field without putting ourselves out of the game?

There is a great deal of unanimity in the world about what the principles are in this area. Look at the new principles of the OECD. More countries took part than the last time and the outcome is surprisingly the same. I see that at international conferences as well. Of course there are differences between APEC and the EU, but there are also similarities. And when it comes to implementation in practice I think that to a large extent we are all moving in the same direction. That also applies to America, even though they are very reluctant there to take a step forward. But do not underestimate the influence which Europe has had and still has in this area.

Therefore, if we can make good use of the moment, that will de facto lead to a world standard with enormous influence. There are all kinds of ways in which to make a standard of this kind interoperable between difference countries. One way is to start

from the assumption that companies want to be compliant but preferably want to implement a system worldwide once, for costs which are as low as possible. We now have that option. And then there is also the formidable market force of Europe. The Federal Trade Commission [FTC] in America has also become far more active in the area of the protection of privacy. Unlike in Europe, in America non-compliance with privacy policy is seen as an unfair trading practice but they actually achieve a great deal on this basis. The FTC has in a number of cases shown itself to be prepared to impose a sanction where something had been promised in Europe but had not been delivered. They did not do that by chance.

There is therefore an increasing willingness to work together with Europe. In the light of the trans-Atlantic market that is a formidable contribution to interoperability. I have sometimes described the European system of *adequacy* as a contribution to interoperability. We are on the eve of a number of important developments. Look, for example, at Google, which is now being investigated in a number of countries. That will probably also give rise to case-law and that is also necessary because our world is becoming ever more integrated.

How should a compliance officer deal with these worldwide differences?

The DPO can ensure that in the context of his organisation he develops an agenda in which these things are dealt with systematically. The DPO must therefore ensure that the (worldwide) requirements are translated in terms of the products and services of his company. Where necessary, small differences will of course be seen between countries and markets but it must be an integrated approach. If you work in an organisation for which it is important that personal data are handled properly and which does not want to run the risk of negative publicity through a data leak or an enforcement action, then you have to invest in it. If enforcement activities increase, then this integrated approach can only become more important and that would be a healthy development.

And how should a supervisor handle this complexity?

It is the task of the controller to comply with the rules. And it is the task of the data subjects to exercise their rights. It is therefore important for the supervisor that the system works well by and large. If the system does not function properly, as the supervisor you have to do something. That also applies if parties misbehave structurally. The supervisor must therefore not concern himself too much with small fry, but the small fry do have to be served. There must therefore be a place you can go, if necessary somewhere else.

The challenge for the supervisor is to continue to focus on the big picture and then step in in time. As the supervisor you must not allow yourself to develop tunnel vision because you are so busy with daily matters such as complaints, notifications etc. As supervisor you must always ask yourself whether you are indeed working on the right things, whether you are really using your scarce resources effectively.

The supervisors argue in favour of more accountability, but in practice frequently still split hairs and give no credit for what is already happening in organisations in the area of privacy management. Will the supervisors succeed

in making this change?

I hope so. A number are doing that already. A European Data Protection Board will also help with this. Ultimately it will become increasingly more consistent but it is a process which is still growing. As the EDPS we are already working in this way. We look where the great risks are with the controllers, such as the content of the information and the way that it is used. Where is it good enough, by and large, and where do we have to keep on top of it because the risks are too great?

Currently the one-stop-shop idea and the proximity principle are a serious obstacle to the progress of the Regulation. But it is not unimportant that a good solution is found for this, not least from the perspective of the DPO who has to advise the organisation about the rules and the risks. How do you view this?

The one-stop-shop idea and the proximity principle are indeed at odds with each other. This is the subject which is currently being talked about a lot and on which the success or failure of the revision project hangs at this stage. In October I think that we were closer to a solution than in December. The subjects must not be seen as being separate from each other. The one-stop-shop idea is an excellent one but you must recognise that there is a one-stop shop for companies and a one-stop shop for data subjects. And as these are different in cross-border situations, you have to accept that there is never just one place to go. The Lead Authority does not have exclusive competence. You therefore have to see it as a form of division of labour. If the Lead Authority is seen as the leader of a team, you are much closer to the solution. And that also applies the other way round. As far as I am concerned, the problem can therefore definitely be solved.

But is it not ultimately simply a matter of money? You do not want every country to be able to impose a fine separately but eyebrows will be raised if the whole fine goes to one country.

Even here you should still be able to do something. If you carry out the idea of cooperation logically, you could even regulate for a fine of this kind of 100 million to be distributed between the countries involved. That is not in the Regulation yet but, if you have to solve this problem, that is the way to do it. But what is more important is that we should ask ourselves what the one-stop shop really is. On the one hand, under the one-stop-shop rule a supervisor has certain tasks; on the other hand he has certain powers which do not accord with those tasks. The French supervisor cannot carry out an on-site investigation in Germany. He has to ask his German colleague to work with him and then you already have cooperation in the area being investigated. You can also work together to ensure obligations are met. The one-stop-shop rule in the Regulation is really a fancy form of cooperation. And that is the solution for proximity too. Trust also plays a role among judges and among supervisors. The controller does not always have to wait a long time for a decision.

In the EDPB we can try to expedite a case. For example, the EDPB should be able to try to reach a position within six months to which everyone adheres. I understand that in the internet age six months is an eternity, but these are such important cases that

a timescale of this kind is justified. The beauty of the proposal was that it had the procedural triggers to ensure that a good decision was reached from the outset. And a supervisor who deviates from the position of the EDPB must explain why he is doing so. A judge will not be quick to agree to that. At the same time our proposal also solved another problem, namely that the Commission had given itself too great a role which everyone was against. The solution was on the table last October but after that there was too much fragmentation when putting it together, as a result of which in December no agreement could be reached. There are all kinds of possible solutions to this problem without having to set up a new body (a pan-European supervisor, ed.) which nobody really wants. The paradox can therefore be solved.

Six months is perhaps acceptable in the case of an investigation or a complaint, but the consistency mechanism also applies for the consultation of the supervisor regarding projects of the controller on which a PIA [privacy impact assessment] has been carried out. And in such cases six months really is a very long time.

Of course in a project of this kind the deadlines must be realistic. A company must not think that they have a good idea and then at the last minute seek approval. Then it is important that you have good advisers who can alert you in good time. Anyway, it is likely that the matters which are obvious and which will in any case be on the agenda will be the first through the consistency mechanism, perhaps even during the Regulation's transition period. At the time when the Regulation enters into force, there will therefore already be guidelines and verified policy on the subjects which come up most frequently. So if a company comes along with a question which is not too outlandish, it will be able to receive an answer reasonably quickly. On that point too you will see a gradual process. But if you are working at European level, you must do it to the right scale.

So the implementation of the Regulation may still vary between countries?

Commissioner Reding calls the Regulation 'one single law everywhere'. I would like to call it 'a single framework law everywhere'. It has become a Regulation with many open areas in important subject areas. And that is necessary because you have to allow the laws of all the 28 Member States to work together with the Regulation. That cannot happen with a dogmatic approach. According to European law, a regulation is very dominant. But it depends on what that regulation says. If this regulation is drawn up in such a way that it makes co-existence possible, then there is no problem. That is what the Council is working on at the moment. In the Regulation there are 'legal obligations', but it does not state which legal obligations. Think, for example, of tax legislation or legislation on occupational health and safety. They are full of legal obligations surrounding the processing of personal data. And if these obligations are compatible with fundamental rights, they can be considered as legal obligations within the meaning of the Regulation. You can therefore leave them to run in parallel. But the Member States have to act in anticipation of the Regulation. Otherwise the legal consequence is that all this local legislation will be replaced on the entry into force of the Regulation. And nobody wants that, so you have to think about the whole thing in detail. I think that the Commission has underestimated that a little.

All things considered, what message do you want to give to our readers?

I would like to start by saying that privacy professionals as such are a growth area and will play a very strategic role in the system. We will need these privacy professionals at all levels. And then not only lawyers, we will also need people with a technical background or with management skills.

Secondly they must not sit on their hands but the risk is that you try to do too much on your own. That's not possible of course and therefore you will have to conceive a plan as a result of which change will nevertheless take place gradually. You will have to be patient and show some imagination. Be comforted by the thought that that is exactly what I had to do when I started here as EDPS with nothing. The fact that we are where we are shows that it can be done. And if you also have the bit of luck you need, you can continue to do that enthusiastically with a whole team.

The third point is that I think that this renewal of the European framework is unavoidable. The date on which that will be completed is currently unclear. Let's be honest, we will not achieve it before the European elections. The end product will also not be the same as what we started with, but something which looks very much like it and is better. We are currently catching up quite a bit and that's not a bad thing. Very many people do not realise how sensitive this subject is or what huge legal questions surround it.

And finally I would also say this: as supervisors we are currently busy acting as bridges between the conventional privacy professionals and all those people who are busy with the development of the internet, software, hardware and standards. Those people have been shocked by the NSA affair. We are going to involve a number of people working in the world of '*privacy-aware internet development'* to try to achieve a multiplier effect. And that shows that supervisors too have to be creative.